Printed & Bound by
Abbey Bookbinding
Unit 3 Clos Menter
Gabalfa Workshops
Western Avenue
Cardiff CF14 3AY
T: +44 (0) 29 2062 3290
F: +44 (0) 29 2062 5420
E: info@bookbindersuk.com
W: www.bookbindersuk.com

THE UTILITY OF ELECTROMAGNETIC ATTACK DETECTION TO INFORMATION SECURITY

RICHARD HOAD

A submission presented in partial fulfilment of the
requirements of the University of Glamorgan/Prifysgol Morgannwg
for the degree of Doctor of Philosophy

This research programme was carried out
in collaboration with QinetiQ Ltd.

December 2007

QinetiQ/07/02208

Abstract

Electromagnetic (EM) threats are a specialised subset of offensive threats to the confidentiality, integrity, and availability of information and to information security (INFOSEC) in general. Two broad classifications of threat types; EM interceptors (interception of compromising Radio Frequency (RF) emissions) and EM disruptors (The use of high power RF to disrupt electronics) have been considered and the technical aspects of these threats have been assessed. The technical complexity amongst other factors required to mount an EM interceptor based attack has been shown by analysis to be significant.

The hypothesis of this thesis has therefore been focussed on the development of detection and diagnostic concepts analogous to those used to defend against conventional cyber or Computer Network Attack (CNA) threats for EM disruptive attacks. EM Disruptors which have been the focus of this study are likely to have a large impact on the *availability* of information systems but it has been shown that the effectiveness of the threat and therefore the risk posed to INFOSEC is extremely difficult to quantify. Nonetheless, it has also been shown through analysis and discussion that the 'Low Tech' perpetrator (well funded amateur) would be likely to be capable of building an effective EM disruption system.

Whilst effective countermeasures for EM disruptors exist it is suggested that it is difficult for INFOSEC professionals to recommend their installation for risk mitigation because the risk is poorly quantified.

A series of rigorous EM susceptibility experiments were conducted on computer systems to identify susceptibility trends and to assist with understanding the risk. A prototype Electromagnetic Disruption Detection System (EMDDS) has also been designed and developed. This detector uses similar principles to cyber type Intrusion Detection Systems (IDS) and should therefore be understandable to non EM specialists. It has been shown that the EMDDS system can be used for responding to incidents and as part of a forensic evidence gathering process.

The results of this thesis have supported the hypothesis.

Table of Contents

List of Figures

List of Tables

Acknowledgement

I would like to acknowledge the support of Prof. Nigel Carter of QinetiQ who acted as my industrial supervisor throughout this study and provided valuable grounding of concepts and ideas.

I would also like to thank my colleagues at QinetiQ for their contributions and encouragement for this work and in particular, Anthony Wraight, Paul Watkins, David Herke, Andrew Lambourne, Adrian Leaver and Brian Kerr.

Finally but perhaps most importantly I would like to thank my wife Rachel for her strong support and encouragement and for keeping my young son Joshua 'busy' so that I could complete this thesis.

This thesis is dedicated to my nephew Tommy.

1 Introduction

Information is a vital intangible quantity which is fundamental at all levels of society. Technology or more precisely the development of micro electronic devices has revolutionised the way that information is communicated, processed, stored, and displayed. We are now undoubtedly dependant on technology at many levels of society.

Information Security (INFOSEC) is a requirement of the modern world and Information Technology (IT) and more specifically computer systems and processes are an essential and integral part of our business and every day lives. Threats to the confidentiality,[1] integrity,[2] or availability[3] of computer systems are extremely undesirable especially if these systems are used for security or safety critical applications. INFOSEC is a process encompassing all aspects of the man/technology interface, and as with any security process it is only as strong as the weakest link in the chain.

'Cyber' or Computer Network Attack (CNA) threats to INFOSEC, dominate the general perception of risks to INFOSEC. Cyber threats are considered here to encompass

[1] Confidentiality – 'Ensuring that information is accessible only to those authorised to have access'
[2] Integrity – 'Safeguarding the accuracy and completeness of information and processing methods'

malicious software, hacking or hacktivism, phreaking, network intrusion, Denial of Service attack, logic bombs and cyber terrorism [Jones and Kovacich, 2002]. The concept can be simplified to any malicious activity where both the source of the threat and the victim system (and perhaps the transport medium) are computer systems.

As an example, consider cyber terrorism where an accepted definition is:

- Terrorist use of computers as a facilitator for their activities
- Terrorism involving computer technology as a weapon or victim [Conway, 2003]

Malicious physical threats to INFOSEC such as criminal malicious damage or theft of property and accidental physical threats such as fire, flood and acts of God are also recognised risk factors.

Important INFOSEC standards have been developed which provide a framework for management of information security. These standards and practices are now well established and both generic standards (IEC 17799), Government guidelines [UKSP01, 2000], and product specific standards now exist [Karygiannis and Owen, 2002]. The generic INFOSEC management standards set out to provide a comprehensive set of controls comprising best practice in information security. The standards are intended as guidance and only recommend INFOSEC process. In the UK strict compliance to these standards is not mandatory.

The assessment of risk is the fundamental principal of the INFOSEC approach used so that balanced and proportionate controls can be put in place [Jones and Ashenden, 2005]. The slightly modified risk model [Wik, 2002] shown in Figure 1 can be used as a guide to understanding the risks to INFOSEC.

[3] Availability – 'Ensuring that authorised users have access to information and associated assets when required' [IEC 17799, 2005]

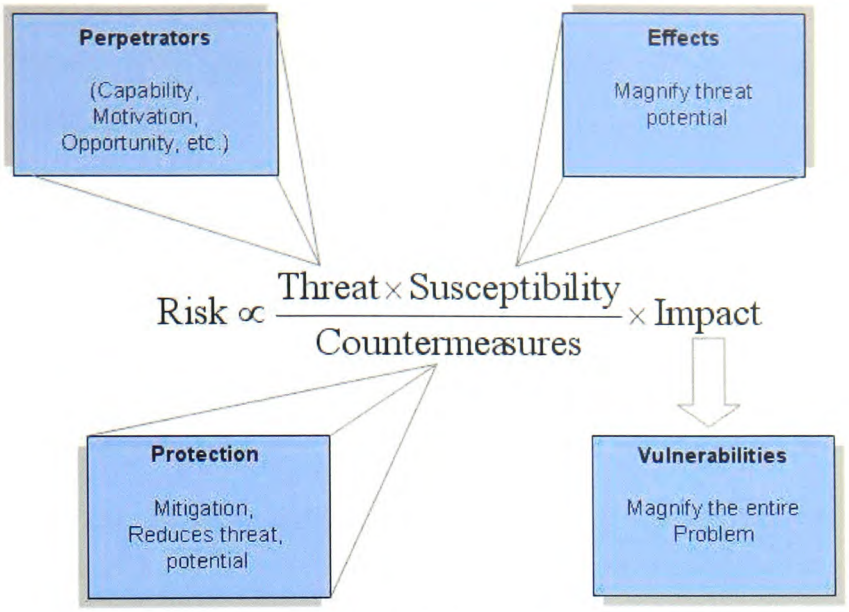


Figure 1: Risk model

This model is not a mathematical expression but provides a clear interpretation of the factors which contribute to the overall risk. The term 'susceptibility' is used to describe any effect to the function, whereas the term 'vulnerabilities' is used to describe susceptibilities which have a detrimental impact on the function. This definition is subtly different to that used by the cyber community and is discussed in more detail is Section 2.1.2.

For many years there has been considerable effort expended in:

- Understanding cyber and physical threats
- Risk analysis of cyber threats, in part through vulnerability and penetration testing
- Providing indication of attack, through intrusion detection systems for example
- Identifying and protecting critical systems, for example with the use of firewalls
- Development of forensic techniques for the diagnosis and hopefully prosecution of perpetrators

Still, 96% of the UK's very large businesses (>500 staff) reported a premeditated and malicious INFOSEC incident during 2005/2006 and the cost of the worst breach was on average £1m to £2m [ISBS, 2008].

Electromagnetic (EM) threats are an emerging and specialised subset of offensive threats to INFOSEC. Electromagnetic threats have been associated with hacker, criminal, terrorist, and information warfare goals such as espionage [Schneier, 2000], [McNamara,

2003], and disruption or damage to information infrastructures [Schwartau, 2000], [Schwartau, 1994], [Wik and Gardner, 1999], [Levien, 2004], [Van Keuren and Wilkenfeld, 1991].

However, EM threats to commercial enterprises do not appear to be explicitly considered as part of the prevalent INFOSEC standards. It is conjectured that this is because the risk posed to business processes by EM threats is poorly understood and compounded by the inability of security professionals to detect and therefore respond and protect processes from this form of attack.

From reviewing open literature discussion about the attractiveness and efficacy of EM threats, it is apparent that the potential risk to INFOSEC from EM threats is centred on:

- Our reliance and dependence on information infrastructures
- The availability of components and the simplicity of constructing systems capable of launching effective EM attacks at all adversarial levels (It has been suggested that the expertise required to build an effective system is less than that required to build a car bomb)
- The increased vulnerability of information infrastructures primarily through the use of technology
- The inadequacy of existing protection measures and the lack of detection devices
- The insidious, remote and covert nature of EM threats. Some authors have asserted that EM weapons are ideal weapons for information warfare

It can be seen that many of these reasons are very similar to the arguments in support of the risk to INFOSEC from cyber type threats. It is therefore postulated that detection of EM threats in a similar manner to detection of cyber threats in the form of Intrusion Detection Systems (IDS), may be a useful tool for assessing risk, providing forensic evidence, and importantly to facilitate fast and proportionate recovery from malicious EM-initiated incidents.

Indeed due to the particular insidious and covert nature of EM threats a correct and timely response to an EM initiated incident is a key challenge.

1.1 Hypothesis and Approach

The hypothesis of this thesis is that:

It is useful and possible to develop detection and diagnostic concepts analogous to those used to defend against conventional cyber or CNA threats for electromagnetic attacks.

1.2 Objectives and Thesis Structure

In order to satisfy the demands of the hypothesis the objectives of this thesis have been broken down into three stages:

Stage I – Understanding the technical feasibility of EM threats

Stage II – Understanding the susceptibility of information systems from EM threats

Stage III – Developing detection concepts which facilitate an effective response to malicious EM initiated incidents

1.2.1 Stage I – Understanding the technical feasibility of EM threats

In this first stage a comprehensive literature review and a subjective threat analysis was undertaken

Objectives:

- Develop an understanding of the basic concepts of EM interaction
- Detail the principles of two EM threat classes
- Understand the features of EM threats
- Understand countermeasures/mitigation of EM threats
- Conduct simple analyses to determine the effectiveness of the different threat classes
- Prioritise threat classes to limit the problem space

Where possible the findings of the initial experiment or study phase have highlighted differences and similarities between EM and Cyber or CNA threat types.

1.2.2 Stage II – Understanding the susceptibility of information systems

In the second stage experiments were conducted in order to further refine an understanding of the threat and to enable the formulation of a requirements specification for EM threat detection.

Objectives:

- Conduct experiments to assess the radiated susceptibility of computer systems
- Conduct experiments to assess the radiated susceptibility of computer networks
- Summarise findings so that detection concepts can be developed

1.2.3 Stage III – EM attack detection and incident response

In the third and final stage one of the concepts was developed into a proof of principle demonstrator.

Objectives:

- Develop detection concepts based on conventional cyber type threats to INFOSEC which are therefore easily understandable to INFOSEC professionals
- Take at least one of these concepts through to a manufactured prototype
- To promote a synergy of understanding between conventional cyber and EM threats
- To postulate how EM detection can be used for forensics and incident response

2 Stage I – The Technical Feasibility of EM Threats

2.1 Basics of Electromagnetic Interaction

2.1.1 Electromagnetic Interference Phenomena

The focus of this work covers the EM phenomena associated with the lower end of the EM spectrum i.e. the Radio Frequency (RF) and microwave regions (a few Hz to a few ten's of GHz (10^9 Hz), Figure 2.

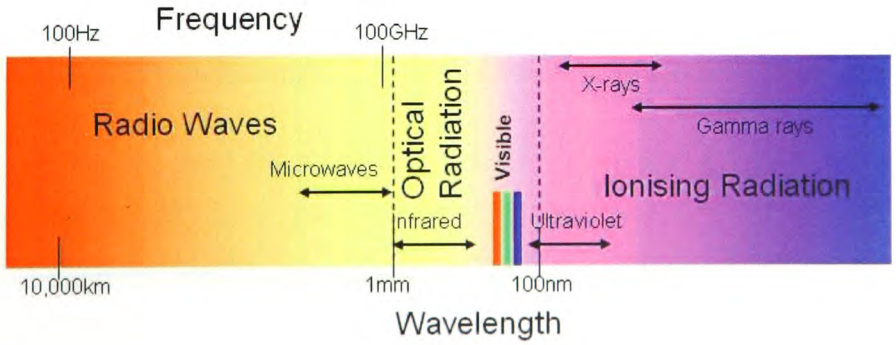


Figure 2: The Electromagnetic Spectrum

All electrical and electronic systems, to some extent, produce and respond to EM phenomena, this factor is exploited to produce RF communications, and telemetry such as mobile telephony, satellite links and radar.

The phenomena of particular interest to this study are related to EM emissions and interference. The IEC definition of EM interference is:

'degradation of the performance of a device, transmission channel or system caused by an electromagnetic disturbance' [IEC 60050-161, 2006].

2.1.2 History of EM interference phenomena

Since the very first experiments in radio communication, conducted by Marconi in the late 1890's interference phenomena have been known to exist. However, technical papers on radio interference only began to emerge in the 1920's [Paul, 1992], coincident with the greater proliferation of radio transmitters and receivers. This was largely a co-channel interference problem since radio regulation of bandwidth was not enforced at this time. It is speculated that the German army intercepted emissions from the Allies on the battlefield as early as the First World War [Young, 2002].

Other natural EM interference phenomena also contributed to the problem at this time. Examples of natural interference sources are lightning (direct and indirect effects, sometimes referred to as Lightning Electromagnetic Pulse (LEMP)), static electricity (Electrostatic Discharge (ESD) and Precipitation static (P-static)).

Later, in the 1930's, radio interference from electrical apparatus such as electric motors, electric railroads, and electric signs began to cause major problems to radio reception. These systems could be termed emission sources or more specifically unintentional interference sources since the electromagnetic disturbance caused by them was not part of their main function. The disturbance was caused by some secondary effect such as harmonics produced by switching electrical arcs or self oscillation in resonant circuits.

Due primarily for the need for world trade, International co-operation on interference began with the formation of two standards committees in 1933. These were the International Electrotechnical Commission (IEC) and the Special Committee on Radio Interference (CISPR).

However, the most significant increases in interference problems occurred with the invention of high density electronic components such as the bipolar transistor (1950's),

integrated circuits (1960's) and the microprocessor chip (1970's). During this period military concerns and requirements provided the thrust for development in this area [Kodali, 2000].

The introduction of semiconductors marked a new phase in the interference phenomena. Electronic circuits not only produced high levels of RF emissions but electrical and electronic circuits which were not receivers were also affected by the interference. The term used to describe electrical and electronic systems which are affected by EM interference is susceptibility, the IEC definition being:

'the inability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance'.

Two significant historical events which identified the potential of using the unintentional emissions from modern systems for espionage are the account by Wright [Wright, 1987] and the demonstration by Van Eck [Van Eck, 1985]. Wright discusses the interception of compromising emissions from the Telex wires of the French Embassy. This intercepted information was reputedly used by the British intelligence service to understand the French position regarding the European Economic Community.

Wim Van Eck, a Dutch telecommunications engineer, first published a paper and then demonstrated interception on the BBC's Tomorrows World television program. Van Eck showed that the video signal from video display units (VDU) when amplified to drive the display (Cathode Ray Tube, CRT) could be detected at significant range.

Two very important historical events which demonstrated the susceptibility of modern systems are the cases of the USS Forrestal [Leach and Alexander, 1995], and the result of a High altitude Nuclear detonation Operation Starfish, conducted by the US in 1962 [Tesche, 1987]. A summary of these two cases is provided below, greater detail and further cases can be obtained in [IEC 61000-1-5, 2004].

"In 1967 off the coast of Vietnam, a Navy jet landing on the aircraft carrier U.S.S. Forrestal experienced the uncommanded release of munitions that struck a fully armed and fuelled fighter on deck. The results were explosions, the deaths of 34 sailors, and severe damage to the carrier and aircraft. This accident was caused by the landing aircraft being illuminated by carrier-based radar. The resulting EMI sent an unwanted signal to the weapons system. Investigations showed that degraded shield termination on the aircraft allowed the radar frequency to interfere with routine operations. As a result

of this case, system level EMC requirements were revised to include special considerations for electro explosive devices."

"The Starfish nuclear device, with a yield of approximately 1 MT, was detonated about 400 km above Johnston Atoll during the night of 8th July 1962. The line of sight distance from the event detonation to the Hawaiian Island of Oahu was approximately 1400 km. On Oahu, problems were noted in the input circuits of radio receivers, surge arresters triggered unexpectedly on an aircraft with a trailing wire antenna, and 30 strings of streetlights reportedly failed simultaneously."

These cases amongst others prompted the military and civil communities to become concerned about system emissions and susceptibility. Hence standards and testing regimes were introduced to try to mitigate these problems. Most of these phenomena are addressed by working towards Electromagnetic Compatibility (EMC). The IEC definition of EMC being:

'the ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment'.

On the 3rd of May 1989 the council of the European communities issued the electromagnetic compatibility (EMC) directive 89/336/EEC [BSI, 2003] as an attempt to address equipment EMC issues.

There are many EMC standards which apply to Information Technology Equipment (ITE) which are the principal victim/receptor systems considered in this thesis. Two product specific standards of interest to this work are [BS EN 55022, 2006] and [BS EN 55024, 1998].

EN 55022 sets limits for the maximum emission level permissible from ITE together with methods of measurement. EN 55024 sets limits for the immunity requirement of ITE.

In essence the EMC directive aims to reduce degradation in performance of equipment and systems by minimising emissions and providing some level of immunity. It can therefore be considered as providing protection to systems from unintentional EMI and perhaps some basic protection from malicious EM threats.

2.1.3 EM interaction – a simple model

At an engineering level all of the EM interference phenomena can be described via the simple source – victim/receptor model [Chatterton and Holden, 1991], Figure 3.

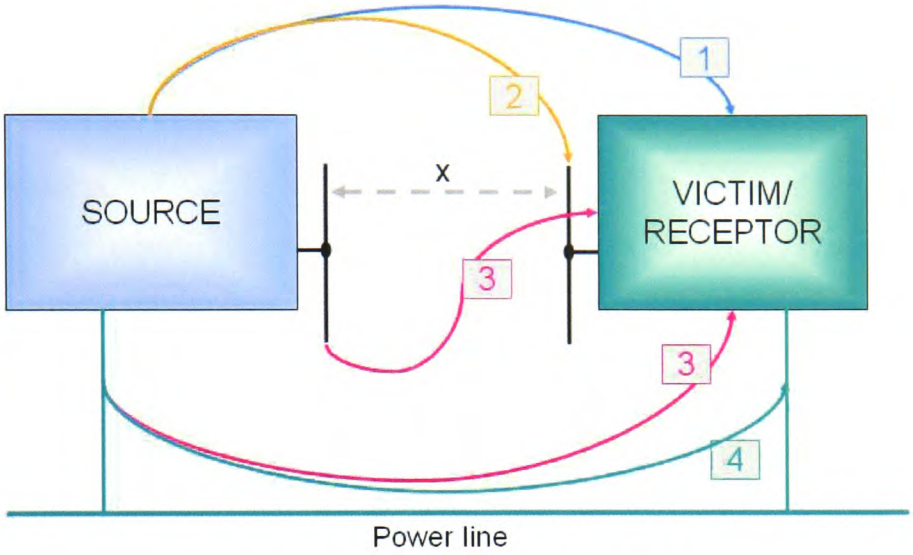


Figure 3: Source – Victim/Receptor model

Sources produce emissions. Emissions, in this context, are RF signals which emanate from the electrical and electronic components. Any conductor can produce these emissions through the movement of electric charges. These emissions if intercepted may reveal information about the source and this could include compromising or confidential information. A source can consist of electrical or electronic system including but not limited to:

- Integrated circuits (IC's)
- Electronic circuits
- Video Display Units (VDU's)
- IT Systems
- Electric motors
- Radio transmitters
- Radar transmitters
- Power Transmission lines

In this diagram the victim/receptor can be susceptible to the emission or other forms of external interference. If the magnitude of interference is high enough all systems will demonstrate susceptibility. Victim systems could consist of:

- IC's
- Electronic circuits
- IT Systems
- Radio receivers
- Domestic appliances

It can be seen from the diagram of Figure 3 that there are several paths from the source to the victim over which EM emissions and interference can propagate.

Path 1: Represents direct radiation from the source to the victim over the air. This is referred to as radiated interference. The emission propagates from the source via apertures, such as fan grille slots or via the system enclosure and enters the victim/receptor via apertures.

Path 2: Is also representative of radiated interference from the source however in this instance the interference is 'picked up' by the victim cabling, such as antenna, power, signal or control cables (e.g. network or keyboard leads). The interference that propagates to the victim/receptor along the cable is termed conducted interference. It should be noted that incorrectly shielded wires, and metallic pipes or conduits can act as an antenna.

Another term used to describe interference coupling to non antenna elements such as apertures, enclosures or cables is 'back door' coupling. This differentiates it from the coupling to actual antennas or electronic sensors, which is known as 'front door' coupling.

Path 3: Interference is radiated from an antenna or cables and couples to the victim/receptor via the aperture or enclosure.

Path 4: This represents a purely conducted disturbance where the emission from the source propagates to the victim through cabling. This cable could be the power line as

shown or in practice any interconnecting cable (e.g. network connection) or conductor (e.g. a copper coolant pipe).

Path x: This path represents actual physical antennas and the source and receptors are specifically transmitting/receiving devices. This path is representative of normal radio communication (e.g. Wireless Local Area Networks (W-LAN), radio broadcast/reception). This distinction between intentional transmission/reception and unintentional transmission and unintentional reception is important and is discussed in more detail in Section 2.1.4.

The actual physical mechanisms of electromagnetics are best approached from an understanding of Maxwell's equations which govern all aspects of electromagnetic phenomena. However, since electromagnetic theory is complex only a brief overview of the pertinent aspects of the phenomena is considered necessary. Discussion concerning some of the underlying physical considerations which apply to EM interaction and the source victim/receptor model in the context of this thesis are discussed in Appendix A.

2.1.4 Malicious Electromagnetic Threat Types

It is not the intention of this work to concentrate on the myriad of subjective factors such as motivation, funding of threat agents, likely events to trigger an attack etc, which constitute threats to real systems [Jones, 2003]. Rather it is the intention of this study to assess whether EM attacks are technically feasible and to assess the risk posed to INFOSEC from a technological standpoint.

Malicious EM threats exploit the coupling paths shown in Figure 3 and discussed in Section 2.1.3, in one of two ways.

1. Interception of compromising emissions from the source, (i.e. emissions that can be decoded to provide information about the system), Figure 4.

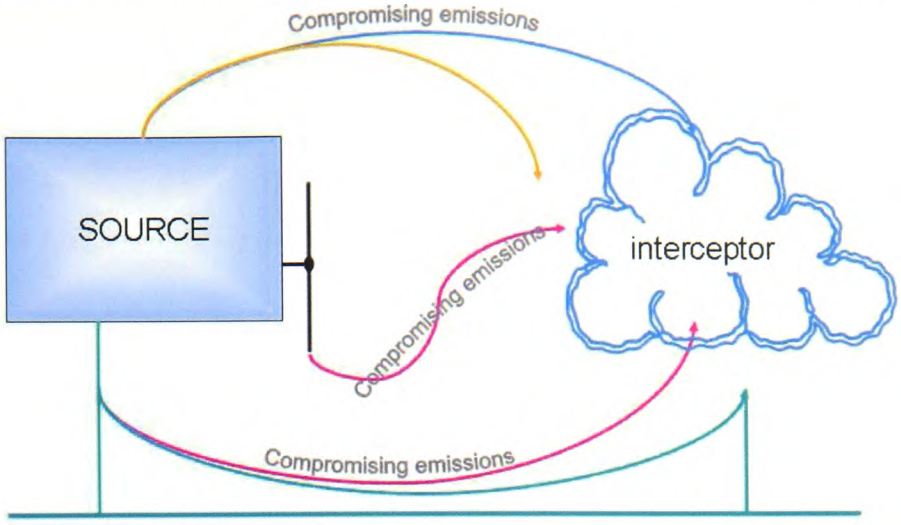


Figure 4: Interceptor model

The EM interceptor threat is broadly comparable with the cyber threat known as spyware [Hackworth, 2005] where it is the perpetrators intention to get unauthorised access to confidential information such as passwords.

2. Disruption of the Victim by generating interference levels above the immunity threshold of electronic systems and thereby exploiting a system susceptibility, Figure 5.

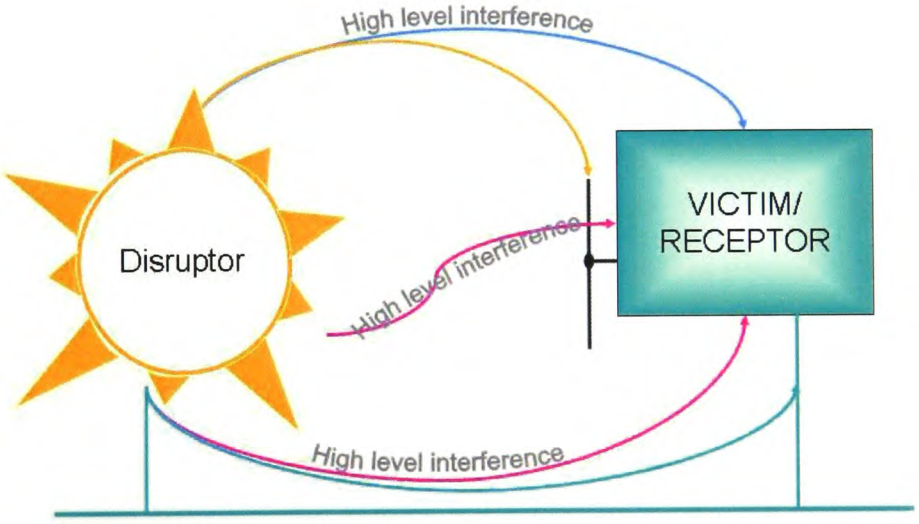


Figure 5: Disruptor model

The disruptor threat is broadly comparable in cyber space with a denial of service attack, except a disruptor is likely to deny service to hardware rather than just a website, software interface or process.

2.1.4.1 Electronic Warfare

A distinction should be made here between the forms of threat described above which form the major part of this thesis and classical Electronic Warfare (EW) and electronic surveillance methods. EW specifically exploits *intentional* transmission and reception i.e. systems and equipment designed to radiate RF and those therefore that have intentional antennas (i.e. Path x, Figure 3). These could be communications systems such as radio broadcast or indeed Wireless Local Area Networks (W-LAN) or non-communications systems such as Radar and radio navigation systems. The EW exploitation of intentional transmission and reception systems is sophisticated in that it is conducted covertly to avoid detection.

This form of threat is not unknown in cyberspace [Silver, 2001], [Potter, 2003], [Woodward, 2004]. Indeed, the terms war driving, wireless jacks and cyber jacks indicate that hacking/assessment tools exist to exploit this particular point of entry into a system [Wepcrack, 2006], [Airsnort, 2006], [Netstumbler, 2006]. These threat types deliberately attack the RF communications channel where the radio frequencies of interest are well known and indeed published in open standards. The principal objectives of the attack are either to intercept information or to deny service to the communications channel (sometimes referred to as jamming).

EW purposefully and specifically exploits the RF communications path via antennas (in-band attack), generally in a covert manner. The main threats considered in this thesis are threats to information systems and process which in general are not deliberate emitters or receivers of RF radiation (out of band attack). However, the boundaries are blurred especially with the integration of low power emitters such as W-LAN, 802.11b, and Bluetooth into the heart of IT systems [Intel, 2006].

In Section 2.2 it is shown that an EM interceptor is capable of capturing any RF communication signals although general RF communication is not in many cases the specific source which is exploited. In Section 2.3 it is shown that EM Disruptors can also be used to intentionally or unintentionally jam, disrupt or even damage RF communications reception.

EM Interceptors and EM Disruptors potentially have the ability to affect the whole range of electrical and electronic technologies which support information systems and processes and are therefore the primary concern of this thesis.

2.1.5 Background Summary

The concept of EM interaction and EM threats to INFOSEC has been introduced. Two broad classes of the threat have been introduced:

EM Interceptors – Possess the capability to capture and exploit compromising RF emissions from information systems and processes. A threat to the confidentiality of information

EM Disruptors – Possess the capability to disrupt and damage electronic technologies which underpin information processes. A threat to the availability of information

Section 2.2 and Section 2.3 discuss interceptor and disruptor concepts in greater detail.

2.2 EM Interception

In the Section 2.1.4 the concept of an EM interception based threat was introduced. The fact that any electrical and electronic system can act as a source which produces electromagnetic emissions was discussed.

2.2.1 Definitions and associated terms

EM Interception has been defined in a variety of different ways which essentially describe the same phenomena.

One definition for this form of threat is:

'The interception of compromising radio frequency (RF) or EM emanations or emissions from electronic equipment' [Buchanan, 2003].

Other terms used or associated with this threat include TEMPEST, Compromising emanations (CE), electronic eavesdropping [McNamara, 2007], Van Eck Radiation, and Unintentional Emissions (UE) detection.

TEMPEST is further defined by the UK Communications and Electronic Security Group (CESG) as:

'The study of the emission of unintentional protectively marked data (usually Confidential and above) from an equipment or system. If these emissions were intercepted and analysed they could reveal compromising emanations and thus the protectively marked data.' [CESG, 2005].

TEMPEST is regarded by some as a military or government agency acronym [NSA, 2001] and has been the subject of much speculation in the civil community as the abundance of unofficial web based articles confirms. The term EMSEC is also used extensively. EMSEC can refer to Emissions or Electromagnetic Security. A definition of EMSEC is:

'The protection resulting from all measures designed to deny unauthorised persons information of value that might be derived from intercept and analysis of compromising emanations from other than crypto-equipment and telecommunications systems' [ITS, 2004].

Clearly this is a very similar definition to the one previously but with a shift in emphasis to protection rather than detection.

Another definition from open source literature was found in a published declassified National Security Agency (NSA) standard [NSA, 2004]. Here the code word TEAPOT is discussed as:

'A short name referring to the investigation, study, and control of intentional compromising emanations (i.e., those that are hostilely induced or provoked) from telecommunications and automated information systems equipment.'

This term appears to imply that backdoors can be introduced to make it easier to carry out an interceptor attack.

2.2.2 Standards

Given the above discussion it is clear that potentially confidential or security classified information may be remotely observed using this method. Interception based threats are therefore of concern to the confidentiality of information and since confidentiality is breached some of the information integrity will be lost.

Government information security groups (such as CESG in the UK and the NSA in the US) have been aware of this issue for some time (since 1918, according to some sources). In particular nationally or militarily sensitive systems continue to be rigorously tested to TEMPEST standards [NSTISSAM, 1992], [AMSG, 2005]. Essentially specific systems are tested and engineered to ensure compromising emissions are well below a detectable level. These levels are classified but are likely to be below the limits specified in the various openly published EMC standards discussed earlier.

2.2.3 Principles of the method

The techniques for intercepting emissions are not new and simple methods can be employed using fairly standard equipment. Referring to the model from of Figure 3, a typical schematic diagram of the concept is given in Figure 6.

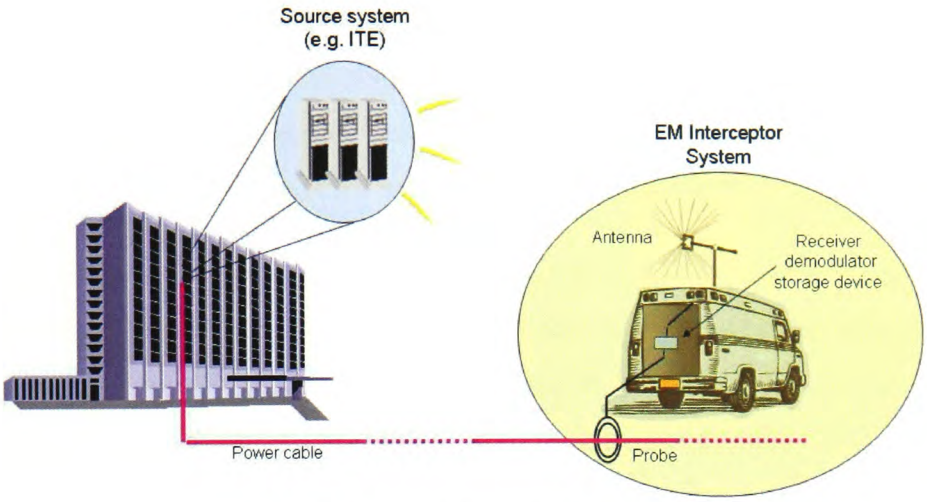


Figure 6: The interceptor threat concept

In this diagram a vehicle containing the necessary reception, processing and storage equipment is used to remotely intercept radiated or conducted RF emissions generated by ITE systems housed within an installation.

2.2.4 Emission sources

The source of the emission can be any form of electrical or electronic system as discussed but of specific importance are those which are used for processing, storing or displaying information which is of unique value to the rightful owner. Examples which are particularly relevant to INFOSEC may include:

- Computer systems including displays
- Network hubs and routers
- Peripherals such as keyboards, mouse and graphics tablets
- Electronic locks
- Access card readers
- Biometric sensors

- Closed Circuit Television (CCTV) cameras

At the circuit board level the source of the emission signal will be a discrete active component such as an operational amplifier. Any current carrying conductor such as a printed circuit board (p.c.b.) trace can act like an antenna [Parker, 1996]. A moving electrical charge in a trace generates an electric current that creates a magnetic field. Time-varying magnetic fields create a transverse orthogonal electric field. RF emissions are a combination of both magnetic and electric fields. These fields propagate from the p.c.b. by either radiated or conducted means as shown in Figure 3.

Digital circuits for example are known to be a source of EM emissions covering a wide frequency range (broad-band). This is due to the fast rising and falling edges of digital waveforms (See Appendix A, Section 6.6). The magnitude of the emission can depend on factors such as, the choice of component, the clock frequency, the circuit layout (i.e. unintentional antennas), and shielding [Robinson, 1998]. For computer systems one study has shown that the primary source of emissions above 1GHz is the Central Processing Unit (CPU) [Radu, 1997].

At the system level the source radiating structure is usually a cable for example the power cable supplying electrical power to the system. With modern ITE several cables can be connected including Mouse, Keyboard, network, or Modem/telephone cables, and these have been shown to be the main antenna structures [Hockanson, 1996]. Apertures on the source system such as fan slots, metal frames, such as Cathode Ray Tube (CRT) housings, and seams can also radiate the RF emission.

When the systems are networked the source of the emission may be formed by ground loops or in the power line return conductor circuit loops.

When the system is considered as part of an installation then re radiation of the emission can occur from other structures such as window frames, concrete reinforcing bars and metal pipes such as those which carry water to sprinkler systems.

A further source is that of intentional RF emitters, such as W-LAN systems, mobile phones etc. which are placed close to sensitive information processing systems. It is very possible for compromising information to 'cross couple' to these intentional RF emitters such that sensitive information is broadcast unintentionally, effectively 'piggy backing' on the communications signal [Anderson, 2008].

According to Figure 6 any cables or other conductors connected to the source system can propagate the RF emission.

2.2.4.1 Compromising Emissions

Whilst RF emissions are well known to propagate from these sources it is only compromising emissions i.e. emissions containing compromising, confidential or otherwise valuable information which are of value to the perpetrator. The terms 'red' and 'black' are used to differentiate between compromising and non compromising emissions respectively. Thus red signals contain compromising information and black signals contain non compromising (e.g. encrypted) information. The compromising information contained within a red signal may be difficult to reconstruct into meaningful data since it is likely to be encoded or possess an indeterminate modulation.

2.2.5 The interceptor system

In the simplest sense all that is required for the interceptor is:

- An antenna - to 'collect' the emission signals
- A receiver – to visualise, measure and perhaps amplify the emission signal
- Some form of signal analysis system - perhaps including a demodulator/decoder, a synchroniser, and processing algorithms to reconstruct and recover the information
- A storage device - to store the intercepted/decoded emission, this could in principle be something simple like a video tape recorder or a computer

According to the earlier model (Figure 3) there is also the possibility of detecting a compromising emission by connecting a suitable probe to a cable and therefore measuring the conducted interference signal. In this case the antenna is replaced by a suitable transducer such as a wire tap or current probe.

An example of a typical emission profile from two typical computer systems is shown in Figure 7. Photographs of the computers under test are shown in Figure 8.

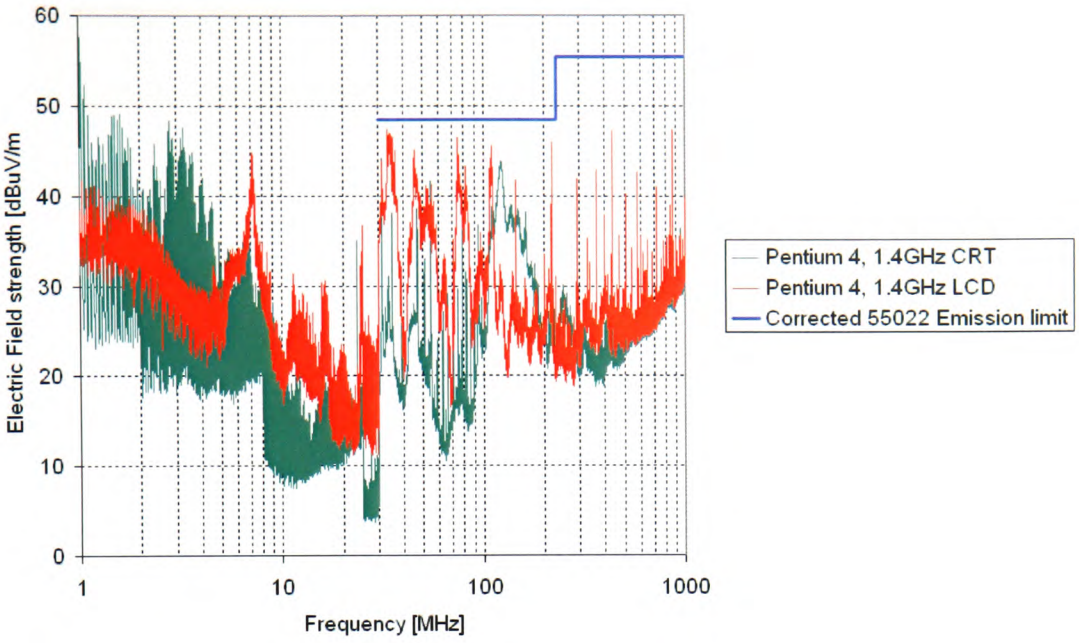
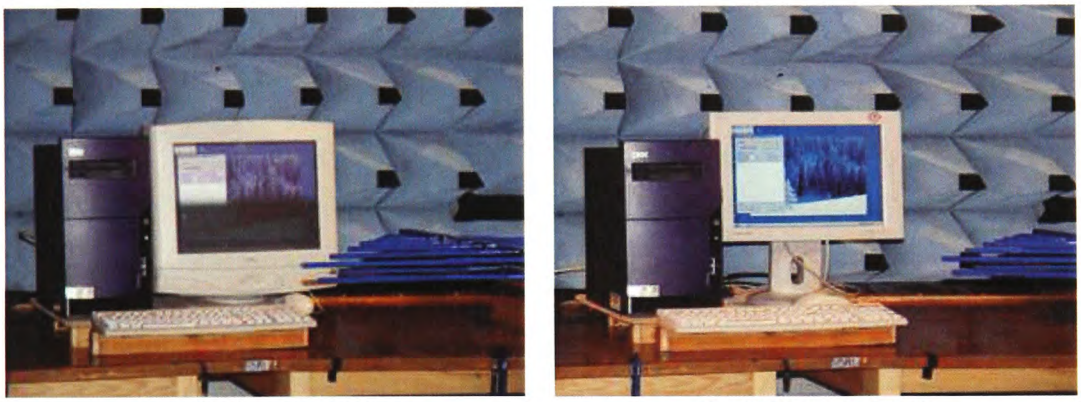


Figure 7: Emission profiles of a standard Pentium 4, 1.4GHz Computer with a CRT and an LCD display



(a) PIV with CRT (b) PIV with LCD

Figure 8: Photographs of a standard Pentium 4, 1.4GHz Computer with a CRT (a) and an LCD display (b) in the test facility

The graph of Figure 7 shows the differences in emission profile with the same computer connected to a CRT and Liquid Crystal Display (LCD) monitor.

This emission profile was measured using a standard EMC emissions test configuration based on Defence Standard 59-41 DRE01 [Def Stan 59-41, 1995]. The equipment used to detect the emission was:

- A Singer-Stodart 41" active Rod antenna (1 to 25 MHz)
- A Chase VBA 6106 Biconical antenna (25 to 200 MHz)
- A Chase UPA 6109 Log-periodic antenna (200MHz to 1 GHz)
- A Rohde and Schwartz ESI EMC receiver (10 kHz Bandwidth 1 to 30 MHz and 100 kHz Bandwidth 30 MHz to 1 GHz)

The measurements were taken in a semi-anechoic shielded room (compliant with the test standard) at a distance of 1 m. Also included on the graph is the corrected emission limit from EN55022 demonstrating that the system measured was compliant with the EMC standard.

The CRT monitor can be seen to have broad band emissions in the frequency ranges 1 to 5 MHz, and 100 to 200 MHz. There are also interesting narrow band 'spikes' in the 30 to 100 MHz band. The same computer with an LCD monitor shows a different characteristic with broad band emissions centred around 7 MHz, 16 MHz, 24 MHz, 36 MHz, 47 MHz, 55 MHz, 75 MHz, 82 MHz, 110 MHz etc. In general the LCD display has emissions of greater magnitude than the CRT display in the frequency bands from 5 to 8 MHz, 10 to 20 MHz, 24 to 96 MHz and from 300 MHz to 1 GHz. However, exactly what the source of these emission 'spikes' and broad band signals is and whether there is any compromising information carried with the emission requires very careful analysis and complex processing.

It is clear from this emission profile that detection of RF emissions at short range is easily achievable using standard EMC type equipment. However, the next stage in the interceptor process is reconstructing meaningful data from the detected emission and this is discussed in Section 2.2.6 by reviewing the open literature.

2.2.6 Interceptors – Open Literature Examples

There are relatively few, peer reviewed scientific or engineering level open literature publications on the topic of the interceptor threat probably because the topic is classified by many nations governments.

The earliest detailed account of interception is given by a Dutch engineer called Wim Van Eck. In this paper Van Eck found that the video signal from Video Display Units (VDU) when amplified to drive the display (CRT) could be detected at significant range

(over 1km). The intercepted signal had to be decoded, demodulated, and synchronised with the source in order to retrieve the information contained. Thus an exact real time copy of the victim VDU could be retrieved at significant distance over the air. Van Eck realised that the emission did not directly emanate from the VDU but was effectively re-radiation from the power cable of the VDU which acts like an antenna. In his paper Van Eck not only described the method but provided circuit diagrams of his system. However, these diagrams were incomplete and were updated in a later article [Highland, 1998]. Van Eck demonstrated the technique on a UK National television programme, the BBC's "Tomorrow's World". Van Eck's form of compromising emission is specific to modulated, wide bandwidth synchronised or rasterised signals typical of video display terminals and is also known as Raster Analysis or RAID [Atkinson, 2006]. These signals have a known frequency and are coherent. It is significant to point out that all of Van Eck's demonstrations and range predictions took place before the introduction of the European EMC directive which mandates a limit on emissions.

In 1989, Bevacqua et al [Bevacqua, 1989] published a paper which attempted to address issues related to the 'TEMPEST problem'. Bevacqua isolated the graphics card oscillator (clock) as the primary source of the compromising emission and provided an outline description of an Interceptor receiver made from 'commercial components'. The paper claims that reception of compromising signals was possible at distances up to 50m. However, the paper is very light on the essential details and no examples are provided. This paper also pre-dates the EMC directive.

In 1990, Smulders [Smulders, 1990], wrote an article about monitoring compromising emissions from computer serial peripheral interface cables based on the RS-232 standard. Smulders showed that 'data signals' could be intercepted at a distance of several metres from the cable even if shielded cable was used. However, Smulders did not demonstrate whether it was possible to recover compromising information from the data signal.

In 1991, Han Fang et al of Tsinghua University, Beijing, China, published a paper which appears to be part of a postdoctoral research thesis [Han Fang, 1991]. Han Fang isolates the emission sources which provide the most compromising information in order of decreasing magnitude as: the video cable, the video display device, the floppy and hard drives. Measurements of the video cable emissions were found to be 40dB above the ambient background environment noise. A basic analytical model is provided, although no details of the measurement system are given.

Sebastiani [Sebastiani, 1998] provides details of the test equipment including instrumentation and shielded anechoic chamber specifications required to conduct TEMPEST testing. Details of some mitigation concepts are also provided, however most of the information is at a superficial level because of claimed security classification issues.

In 2002 the Chinese published another paper on the interceptor topic [Shiwei Dong, 2002]. The primary emission source in this paper is identified as the CRT electron beam although it is claimed that useful synchronisation signals can be detected by the display deflection coils emissions. The paper hints at techniques which could be employed to reconstruct information from the intercepted signal but only provides superficial detail. A crude example is given.

The PhD thesis of Markus G. Kuhn [Kuhn, 2003] is perhaps the most detailed published account of the interceptor threat to date. In this document Kuhn explores the feasibility of interceptor attacks on a variety of types of computer display systems. This study is perhaps more relevant than some of the earlier references since it has been conducted after the introduction of the EMC directive and with modern technology. As discussed previously before the introduction of the EMC directive there were no controls on the level of emissions produced by equipment. Subsequent to the introduction of the directive in the early 1990's equipment emissions were required to be controlled and comply with an emission limit.

In his thesis Kuhn demonstrates the feasibility of mounting an interceptor attack on both analogue (CRT) and digital (LCD) displays. The thesis discusses the instrumentation, measurements, procedures and concepts used for the quantitative evaluation of compromising emissions.

Kuhn shows in some detail how to detect and more importantly recover information from an emission. Three separate demonstrations of the techniques used are provided. The subjects of the experiments are:

- An analogue CRT display connected to a Laptop computer
- A digital LCD monitor which is incorporated within the Laptop
- A digital flat panel display

The instrumentation used included:

- A Log periodic antenna with an Antenna Factor of approximately 22dB/m in the UHF band
- A Dynamic Sciences Inc. DS-1250 specialist TEMPEST receiver[4] set to a very wide video bandwidth (typically 50MHz or greater)
- A high quality, high stability signal generator for the generation of synchronisation signals
- An oscilloscope to carry out multiple captures of radio frequency emission to enable averaging
- Specialist custom built software algorithms that carry out pattern recognition in order to reconstruct the plaintext image from the captured emission

In addition to these instrumentation requirements it appears that it was necessary to have a detailed understanding of the system which was the eventual victim of the attack. In particular the type of video interface used and an understanding of the standards required to develop the video protocol.

For the analogue CRT display reconstruction of the intercepted signal was shown at a distance of 3 m. In this case it was necessary to connect a cable between the receiver and the video synchronisation output of the victim display in order to stabilise the synchronisation. This appears to have been necessary due to limitations in the instrumentation available, in that the synchronisation would drift outside the required limits during the frame averaging time. The period required to complete averaging with the instrumentation used was 10 minutes. In the case of a real interceptor attack it is likely to be unrealistic to attach a cable to the system which is to be the victim of the attack. This could effectively invalidate the advantages of the attack method.

For the digital Laptop display reconstruction of the intercepted signal was shown at 10 m with the victim display in a room separated from the interceptor. The attenuation of the plasterboard wall construction between the rooms was found to be 2-3 dB (see Appendix A, Section 6.3). In this case it was necessary to analyse the source of the emission by probing the hardware in order to understand how to reconstruct the image from the

signal. This was achieved by connecting an oscilloscope directly to a cable within the laptop and varying colours and contrasts to find out how the pixel colour and pattern related to the emission. For the actual demonstration this cable was disconnected and synchronisation was achieved over the air. For a real perpetrator of an interceptor attack this implies that very specific knowledge of the victim system is required for a successful intercept to be accomplished. A custom written algorithm was used to cross correlate the first and last frame in the captured series.

For the digital flat panel display reconstruction of the intercepted signal was shown at a distance of 3 m. A detailed understanding of the Transition Minimised Differential Signalling (TMDS) link protocol (which is utilised by the display type) was necessary in order to reconstruct the signal.

In all of the cases above plaintext was used on the victim display. This text has a high differentiation between the text and the background. It is shown that different foreground background colour combinations and contrasts can make reconstruction more difficult.

It is clear from the discussions above that detection of RF emissions is fairly trivial but reconstruction requires detailed knowledge of the victim system and technical skill. Given the above discussion the level of sophistication, expertise, insider knowledge and time required to mount an effective interceptor attack is considered to be non trivial.

It should be pointed out that the emission phenomena are not restricted to display systems but are common to any digital electronic system as discussed previously. However, no open source information could be found which explored interception from other sources in any detail. It is possible to speculate that interception and reconstruction of emissions from other sources such as microprocessors for example would require a significant understanding of the protocol and message format employed.

Finally, no open source information could be found which exploited the conducting channel (cables etc.) as a propagation path to mount an EM interception attack.

2.2.7 Interceptor Analysis

It has been shown that it is not difficult or impractical to detect emissions from information processing systems. The detection of emissions is routinely performed

[4] The sales of these receivers are the subject of strict controls such that only users authorised by National security agencies are able to purchase and use them.

during EMC testing of equipment at ranges up to 10 m. If we consider Kuhn's most successful demonstration, interception and recovery of data from the laptop display then we can attempt to quantify the maximum effective range for detection.

In Kuhn's demonstration the available signal strength ($Tx_{available}$) = 39 dBμV/m at 10 m in a 50 MHz bandwidth. The actual measured signal amplitude is quoted as 12 μV or 21.6 dBμV. This implies an antenna factor (see Appendix A, Section 6.4.2) of 17.4 dB/m, from Equation 1.

$$A_F = Tx_{available} - Rx_{signal} \quad \text{.....(Eq. 1)}$$

Where, Rx_{signal} is the measured signal level from the base of the antenna in dBμV.

The receiver noise floor appears from the results to be at approximately 3 μV or 10 dBμV. The Dynamic Sciences DSI – 1250 TEMPEST receiver [DSI, 2004] has a quoted receiver sensitivity of 6 dB above Johnson noise. The Johnson noise, which is also known as thermal and white noise level can be found using Equation 2 [Kennedy, 1985].

$$V_n = \sqrt{4kT\Delta fR} \quad \text{.....(Eq. 2)}$$

Where, V_n is the noise voltage

K is the Boltzman constant (1.38×10^{-23} Joules)

T is the absolute temperature in Kelvin

Δf is the measurement bandwidth

R is the receiver impedance in Ohms

If we assume normal ambient temperature conditions of 18 °C, and a receiver input impedance of 50 Ω, then the Johnson noise in a 50 MHz bandwidth is 6 μV or 16 dBμV. The absolute noise floor of the receiver is therefore, 6 dB + 16 dBμV = 22 dBμV. This of course assumes that there are no other environmental man made noise sources in proximity of the receiver.

From [ITU-R P.372, 2001] the environmental noise floor in a business area is 26 dBμV/m at the frequency of interest (75 MHz) in a 1 MHz bandwidth. In the 50 MHz bandwidth used this equates to a noise floor of 43 dBμV/m. By rearranging Equation 1, the noise signal in the receiver is 25.6 dBμV.

Since in his experiment Kuhn has a noise floor of 10 dBμV this indicates that either some form of signal pre-conditioning was used (i.e. a low noise preamplifier) or cross correlation and averaging have been used to improve the signal to noise ratio by a factor of around 16 dB. It is likely that a combination of these elements was necessary.

By assuming that a 10 dB signal to noise ratio is required for successful interception and based on the recorded noise floor we can estimate the maximum expected detection range. We can assume that the interceptor is in the 'far field' region away from the source of the emission since the criterion for the far field boundary (see Appendix A, Section 6.2.2) is met for this frequency. Assuming free space propagation path loss (see Appendix A, Section 6.2.1) the maximum range for interception can be predicted.

The graph of Figure 9 therefore shows the predicted maximum range assuming that the same processing techniques are used and that additional physical barriers do not provide any additional bulk attenuation.

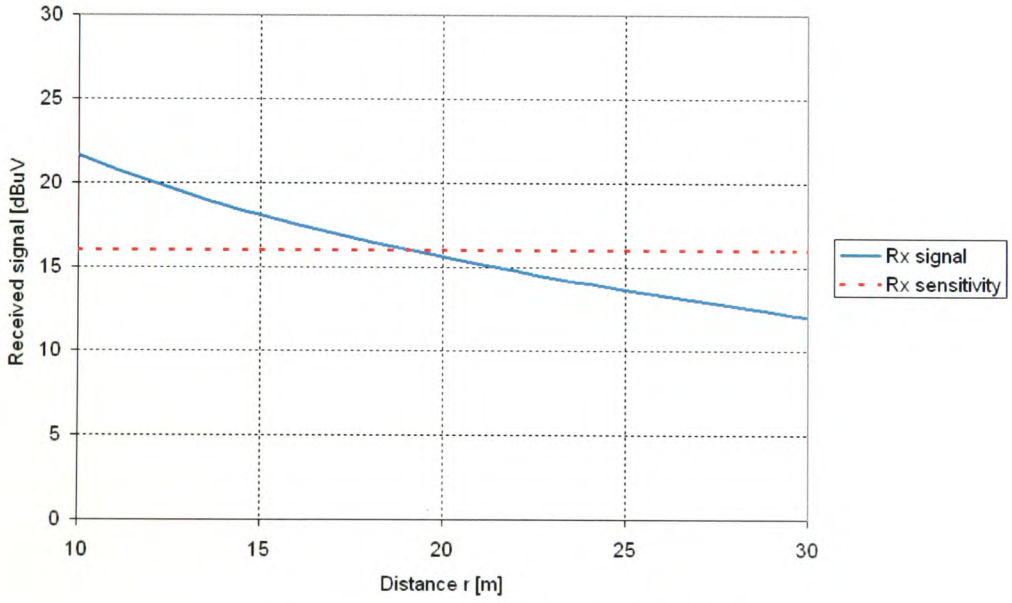


Figure 9: Predicted distance of interception

This shows that the predicted maximum detection range of the demonstration by Kuhn is approximately 20 m. If a greater level of signal pre-conditioning or further averages and

cross correlation were used it would be possible to improve this figure marginally but more capture and processing time would be required.

However, if the barrier attenuation was greater than the 2-3 dB measured or any of the mitigation methods described above were used then the detection range would be significantly reduced. For example a thick concrete wall with an attenuation of just 8-9 dB (see Appendix A, Section 6.3) would reduce the effective range by half.

2.2.8 Interception verses War driving.

It may be useful to compare the technical complexities of interceptor threats with threats to W-LAN such as war driving, drive by hacking and wireless 'jacking' etc.

From the war driver's point of view:

- The receiver equipment required to intercept a W-LAN transmission is standard off the shelf package (e.g. PDA with W-LAN card), routinely available
- Operating this equipment in an office environment would not appear obvious and therefore would not draw unwanted attention allowing range and time advantages
- The source, format and protocol of the intercepted signal are well characterised/standardised since the object of the interception is a communications signal
- Freeware tools are available to crack encryption (if necessary) and reconstruct meaningful information from the intercepted signal such as packet sniffers

For an EM interceptor:

- The receiver equipment required is likely to be specialised or custom modified equipment with a wide bandwidth capability required for impulse detection. Other equipment such as oscilloscopes, signal generators, storage and processing facilities are necessary in some form
- Due to the quantity of equipment required, carrying out an EM interceptor attack outside of the victim installation, perhaps from a van parked in the street or an accompanying office building is the most viable option to minimise suspicion

- Time and patience are required to successfully capture, cross correlate and time average the intercepted data to enable reconstruction of the RF emission into meaningful data

- It is not likely that the source of the emission can be interpreted purely from the intercepted signal. A specific victim must therefore be aimed at. Once the source is defined, intelligence concerning the format or protocol used must be gathered in order to develop reconstruction algorithms

- To the authors knowledge no software tools are explicitly available for reconstruction of information from non-communications emissions

Another important factor is that in either case useful information may not be intercepted. It is likely to take significant time an effort to sift the data for any useful information. For the interceptor this time is magnified by the need to reconstruct data from the intercepted emission.

2.2.9 Forensic Features of Interception based Threats

A very unique feature of an EM interception attack is that it will be invisible to the information system which is the victim of the attack i.e. because of the passive nature of the attack there will be no evidence of the attack at the scene of the incident. Those in rightful possession of confidential information will have no knowledge or sensation that the confidentiality has been breached perhaps until the information is revealed for surreptitious purposes such as blackmail. Indeed the interceptor provides many of the required parameters for a near perfect weapon for an information warrior; it is invisible, passive and insidious.

This form of threat to INFOSEC therefore is unlike many cyber/CNA type threats or physical threats from insiders. Physical threats will leave some form of evidence, unauthorised opening of computer files, loss of data, unauthorised reproduction of material, even fingerprints at the scene of the incident. If INFOSEC procedures are followed cyber/CNA threats such as spyware for example which attempts unauthorised download from a remote link, or even installation of malicious software should also be detected and evidence should therefore be obtainable from the scene of the incident.

2.2.10 Mitigation/Countermeasures

Some mitigation methods, specifically for the interceptor threat have been suggested in the literature. A good reference which covers most of the system design techniques is given by Bai Tungyun [Bai Tungyun, 1997]. These and other techniques are listed below:

- Physically separating classified information (Red) systems from unclassified (Black) information bearing systems
- Zoning of systems
- The use of fibre optics to replace copper cables removing unintentional antennas [Kline, 1991]
- Shielding the source of the compromising emission [Knobloch, 1998], [Bevacqua, 1989]
- Testing of systems to assess the level of compromising emission and then advising on design changes to reduce the emission (TEMPEST testing).
- Altering the software to display low emission fonts, so called 'soft' TEMPEST [Kuhn, 1998], [Junjie, 2001]

Implementation of a physical security barrier or some form of non electronic perimeter control would also be very effective since the magnitude of the compromising emission diminishes with distance from the source.

It should be noted that many of these mitigation measures would provide some protection from the disruptor threat through reciprocity.

Methods for the detection and evidence collection of an EM interceptor based attack do not appear to exist in the public domain. The emphasis for security agencies appears to be in reducing the compromising emission to a practically undetectable or at least unrecoverable level.

2.2.11 Interceptor Summary

It is not difficult or impractical to detect radiated or even conducted emissions from information processing systems at close range. These measurements are carried out for all types of information processing systems as part of EMC compliance. The skill and

challenge for the interceptor lies in the problem of reconstructing meaningful data from the intercepted signal.

All of Van Eck's experiments were conducted before the introduction of the European EMC directive which mandates strenuous emission limits. Even though the emission signal levels measured by Van Eck are not given it seems likely that the detection range postulated by Van Eck (in the order of kilometres) would not be possible today due to emission limit constraints.

Kuhn has shown that detection and reconstruction of intercepted emissions from both modern (post EMC) digital and analogue display systems is possible even in an office environment where there are a number of systems of similar types polluting the spectrum. It has been shown by analysis however, that the range where detection and reconstruction is possible is limited to a few tens of metres. Very sophisticated techniques, relatively sophisticated instrumentation, intelligence of the victim system, and a great deal of technical skill and patience are required to recover the information.

Some articles assert that the complexity of developing and mounting an EM interceptor based attack is great. Further, a review of US National security policy for the secretary of defence, William J. Perry in 1994 [Smith, 1994] states that:

'In 1991, a CIA Inspector General report called for an Intelligence community review of domestic TEMPEST requirements based on threat. The outcome suggests that hundreds of millions of dollars have been spent on protecting a vulnerability that had a very low probability of exploitation.....The rationale is that a foreign government would not be likely to risk a TEMPEST collection operation not under their control.'

The report went on to recommend that domestic TEMPEST countermeasures should only be employed in response to a specific threat. This document appears to imply that non domestic or overseas government offices such as Embassies still require TEMPEST protection.

Military and government departments appear to have a more relaxed attitude to interceptor threats probably because of several factors including:

- The introduction of EM emissions limits such as those required for the European EMC directive

- The time required to mount an interceptor attack
- The proximity required to mount an attack
- The need for insider information about the system in use
- The need to develop decoding algorithms to reconstruct data
- The availability of cryptographic equipment to process confidential information
- The overall technical complexity of recovering compromising information

From the level of complexity described above it seems clear that only very well resourced individuals or groups (such as Nation State Actors (NSA)) could mount a successful interceptor attack. However, three areas of continued concern are likely to be:

1. The increasing complexity, flexibility and availability of low cost receivers, such as software reconfigurable radios, and wide bandwidth communications receivers
2. If effective stimulation of the information system to increase the magnitude or chance of recovery of compromising emission is possible by an insider, or some external influence
3. If confidential compromising information 'cross couples' to uncontrolled transmitting equipment, which is likely to increase the interception range

Point 3 is likely to be of particular concern since the trend in office environments is towards the use of wireless transmitter equipment such as W-LAN, Bluetooth etc.

Due to the technical complexity of the threat type the risk posed to commercial enterprises is likely to be low even though the impact could be very severe. For these reasons and others discussed above this thesis will mainly concentrate on the EM disruptor threat. It will be shown in Section 2.3 that it is perhaps far easier to mount a disruptor based attack and that the impact of disruption is of more immediate concern to INFOSEC.

2.3 EM Disruption - Overview

In Section 2.1.4 the concept of an EM disruptor based threat was introduced. The fact that all electrical and electronic systems are potentially susceptible to electromagnetic interference was also discussed. This form of threat exploits the reciprocal condition of the EM interceptor threat. That is any source which produces emissions is efficient in receiving EM energy via reciprocity (see Appendix A). By employing high power RF transmitters it is possible to couple RF energy into victim systems and potentially cause disruption and damage.

2.3.1 Historical Perspectives

It is not clear when the concept of EM disruption was conceived although the first discussions concerning an RF 'death ray' are associated with Nikolai Tesla. Tesla attempted to build a very high power RF transmitting station at Wardenclyffe, NY, USA [Seifer, 1998] for long range radio communications. Later in 1940 when Tesla was 84 years old he discussed the concept of a disruptor weapon with a journalist from the New York Times [New York Times, 1940]. Tesla's invention the 'magnifying transformer' or Tesla transformer is still used in some of the EM disruptor designs of today.

After Tesla, the concept returned to the science fiction domain since no technology was available to build a disruptor system. In the Second World War with the advent of Radar and the proliferation of long range radio communications high power transmitter technology started to become available for military use.

During the cold war there is significant evidence to suggest that the Former Soviet Union (FSU) researched disruptor concepts which apparently resulted from their recognition that they could not match the capability of Western electronics and that this could be a potential vulnerability for the West. [Schweitzer, 1997].

An unpredicted side effect of the 1962 Starfish high altitude nuclear test which was discussed in the introduction was the disruption, damage and power outage of electrical systems in Oahu, Hawaii, attributed to an Electromagnetic Pulse (EMP). This disruption prompted a great deal of research into EMP phenomena especially in the areas of hardening and protection of military equipment and systems.

The EMP in this instance was produced by a nuclear weapon detonation high in the Earths atmosphere (>30km, so called exo-atmospheric). Exo-atmospheric nuclear

detonations generate ionising radiation that interacts with the Earth's atmosphere causing the generation of scattered Compton electrons. It is the propagation of these electrons through the atmosphere that generates a virtual antenna producing the HEMP that covers several thousand square kilometres at the ground. This wide coverage of a very large area is very different to the other EM threat types listed

In order to effectively test system susceptibility to the perceived EMP threat, EMP simulators were built. Perhaps the largest example of an EMP simulator was the TRESTLE facility at Kirtland Air Force Base, New Mexico, USA shown in Figure 10.

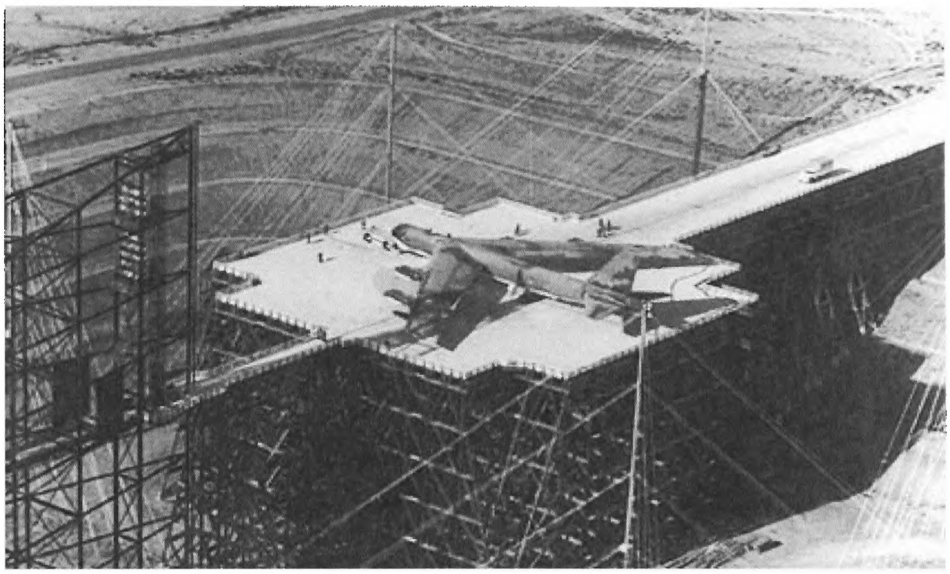


Figure 10: The Trestle EMP facility

TRESTLE was the largest wood and glue structure in the world, the actual EMP pulse generator hardware is off picture at the bottom of the image.

In order to generate a *simulated* EMP event using non nuclear methods and indeed other nuclear weapons effects it was necessary to develop pulsed power sources. Pulsed power became a dedicated field of research which began around 1960 [Smith and Aslin, 1978]. The goal of pulsed power designers was to produce efficient pulsed power machines to drive a variety of sources including Electromagnetic launchers, Laser systems, and X-ray machines.

However, the advent of the USS Forrestal disaster in 1967 also discussed in the introduction is likely to have sparked military interest in EM disruption. Hardening and protection of military systems would have been the primary driver although it is likely that the effects encountered on Forrestal would have been a catalyst for some of the military to consider the advantageous offensive use of EM disruption.

International conferences and meetings which discussed topics such as pulsed power and high power microwave sources and effects began some time after this event. A series of European and American Electromagnetics conferences (EUROEM and AMEREM), and the IEEE Pulsed power conference series have been discussing aspects of disruptor technology for over 20 years. The US National Radio science organisation and the International Union of Radio Science (URSI), Commission E hosted several meetings of the High Power Electromagnetics working group which discussed all aspects of disruptor phenomena including lethality in 1995, 1996, and 1997 [Gardner, 1997].

Around 1996 further impetus to the research field was provided when FSU scientists openly discussed explosively driven disruptor systems. The leading protagonist in the area appears to be Dr. Prishipenko [Merritt, 1998].

In 1997 URSI and the IEC Sub committee SC 77C started to develop standards concerning Intentional EMI (IEMI), an alternate name for malicious EM disruption, although this committee had already been developing standards and advice concerning EMP threats and mitigation to the civil community since 1980.

In 1991, 1997 and 1998 the Joint Economic Committee (JEC) of the United States Senate held hearings concerning Radio Frequency Weapons and the infrastructure [Saxton, 1998]. In 1997 and twice in 1999 the US Congress held hearings concerning the issue of Electromagnetic pulse threats to US infrastructure [Weldon, 1997], [Bartlett, 1999].

At EMC Zurich in 1999 a Workshop titled 'Electromagnetic Terrorism and adverse effects of High Power Electromagnetic Environments' was held which included five papers on the topic.

In 2004 the US has undertook a major re-evaluation of the US critical National infrastructure susceptibility to Nuclear EMP effects. [Graham, 2004]. Threat assessments for EM disruptors have also been provided to the US Congress [Wilson, 2004]. In August 2004 the IEEE published a special issue with over 20 papers discussing aspects of IEMI [Radasky, 2004] and special sessions on IEMI continue to be an integral part of the EMC IEEE and EMC Zurich conference series.

2.3.2 Definitions and Associated Terms

Various terms are used to describe facets of the disruptor threat, and include, but are not limited to:

- Intentional Electromagnetic interference (IEMI)
- High Power Electromagnetics (HPEM)
- Electromagnetic Pulse (EMP)
- High Energy Radiated Fields (HERF)
- Radio Frequency Weapons (RFW)
- Directed Energy Weapons (DEW)
- Non Nuclear Electromagnetic Pulse (NNEMP or N^2EMP)
- Radio Frequency Munitions (RFM)
- High Power Microwaves (HPM), - Hypoband
- Ultra Wide band (UWB), - Hyperband
- Damped sinusoid (DS), - Mesoband

The differences in the terms above describe some differences in the actual mechanism or deployment scenario for the threat. IEMI, RFW, DEW, HERF, and HPEM have been used to describe the general concept of using EM energy for disruption of electronic systems, networks and infrastructures. RFW and DEW seem to be the favoured terms of the military community, although DEW can also encompass Laser based weapons. Whereas, the terms EMP, HPM, UWB, and Damped Sinusoid are generally used to describe the actual EM signature or output waveform of the disruptor.

IEMI and HPEM are terms used by IEC SC77C which deals with high power transient phenomena. The definition of IEMI is:

'Intentional malicious generation of electromagnetic energy introducing noise or signals into electrical and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes.'

A term used by the military and law enforcement communities is Non Lethal Weapons (NLW). NLW encompasses many different techniques for waging non lethal warfare, EM disruption is a small sub set of NLW but the term NLW appears to be less contentious than some of the other terms.

EMP is generally used to describe a single intense pulse of electromagnetic energy. It is frequently associated with nuclear weapons as Nuclear EMP (NEMP) or High altitude EMP (HEMP). EMP produces instantaneous wide frequency coverage dependent on the pulse parameters. The term EMP can also be associated with the radiated disturbance from Lightning (LEMP). N^2EMP is a term initially used by the HPEM community to describe non nuclear means of simulating the VHF induced transient response of cables exposed to HEMP.

RFM is a term used to describe an explosively driven EM disruptor. In this way the explosive energy is somehow converted or modified into EM energy or used to provide electrical power to microwave modulators. Other terms used to describe this RFM concept include E-bomb [Kopp, 1996], Lightning bomb or EMP/T bomb. Associated technical terms relating to the actual generation mechanism include Magneto Cumulative Generators (MCG), Flux Compression Generators (FCG) and Magneto Hydrodynamic devices (MHD).

HPM [Barker and Scamiloglu, 2001] is also known as narrowband [Prather, 2004]. Hypoband [IEC 61000-2-13, 2003] is a standardised term used by the IEC to describe this waveform. Hypoband waveforms comprise of a narrow bandwidth EM signal in the microwave frequency band (above 500MHz). However, there appears to be some confusion since in some circles HPM has been applied to all forms of disruptor technology [Walling, 2000]. Hypoband waveforms can be considered as similar to Radar waveforms. Generally they appear as a train of pulses at some repetition frequency, each pulse contains a burst of a fixed frequency.

The term UWB was initially used by the HPEM community[5]. However the IEC have now created a standardised term, Hyperband, which more accurately characterises UWB like waveforms. Terms such as Transient Electromagnetic Devices (TED) and 'impulse' or 'spike' generators have been associated with this waveform type. Hyperband signals have a very narrow pulse width but have a characteristic high peak level. The 'spike' may be reproduced many times to form a train of pulses at some repetition frequency. In the frequency domain this appears as a very broad bandwidth at low amplitude because the energy is spread across a wide frequency range.

[5] UWB is also associated with a new communications modulation scheme and is used in some Ground Penetrating Radar (GPR) applications for example archaeology or mine detection. However, these applications require different parameters from the UWB waveform than those required for disruptors.

The term Mesoband, a standardised term developed by the IEC more accurately describes DS type waveforms. In the time domain these signal types appear as a damped ringing waveform. This can be reproduced to form a train of damped sinusoids at some repetition frequency. In the frequency domain DS waveforms have a broad energy content due to harmonics produced in the fundamental frequency. Due in part to the techniques used to generate damped sinusoids the centre frequency is generally below the microwave band and can be centred around the lower VHF band up to the microwave band (30MHz to 500MHz approximately). Mesoband waveforms with centre frequencies in the VHF range can also be injected on cables to simulate the induced effects of EMP for susceptibility testing of electronic equipment [McConnell, 1989].

The IEC definitions for waveform classification stem from the diversity of waveforms which can be produced by disruptor systems and the inadequacy of other descriptions. The definitions are based around the frequency contributions of the waveform types and were first postulated by Giri [Giri, 2002]. Table 1 shows how the definitions are derived.

Classifier	**Percent bandwidth (pbw)**	**Band ratio (br)**
Hypoband or narrowband	$< 1\%$	< 1.01
Mesoband	$1\% < pbw \leq 100\%$	$1.01 < br \leq 3$
Sub-Hyperband	$100\% < pbw < 163.4\%$	$3 < br \leq 10$
Hyperband	$163.4\% < pbw < 200\%$	$br \geq 10$

Table 1: IEC classification based on band ratio

Band ratio is defined as the ratio of the highest and lowest frequency content of the waveform at 3dB down from the peak, Equation 3:

$$br = {f_h}/{f_l} \quad \text{.....(Eq. 3)}$$

Where, f_h is the upper frequency where the amplitude is -3 dB of peak

And f_l is the lower frequency where the amplitude is -3 dB of peak

Percent bandwidth is then defined by Equation 4:

$$pbw = 200\left[{(br-1)}/{(br+1)}\right] \quad \text{.....(Eq. 4)}$$

It should be noted that in most cases it is the technology and components used which primarily influence the type of waveform produced by the disruptor. Figure 11 shows the time domain representation for a single pulse of each waveform type.

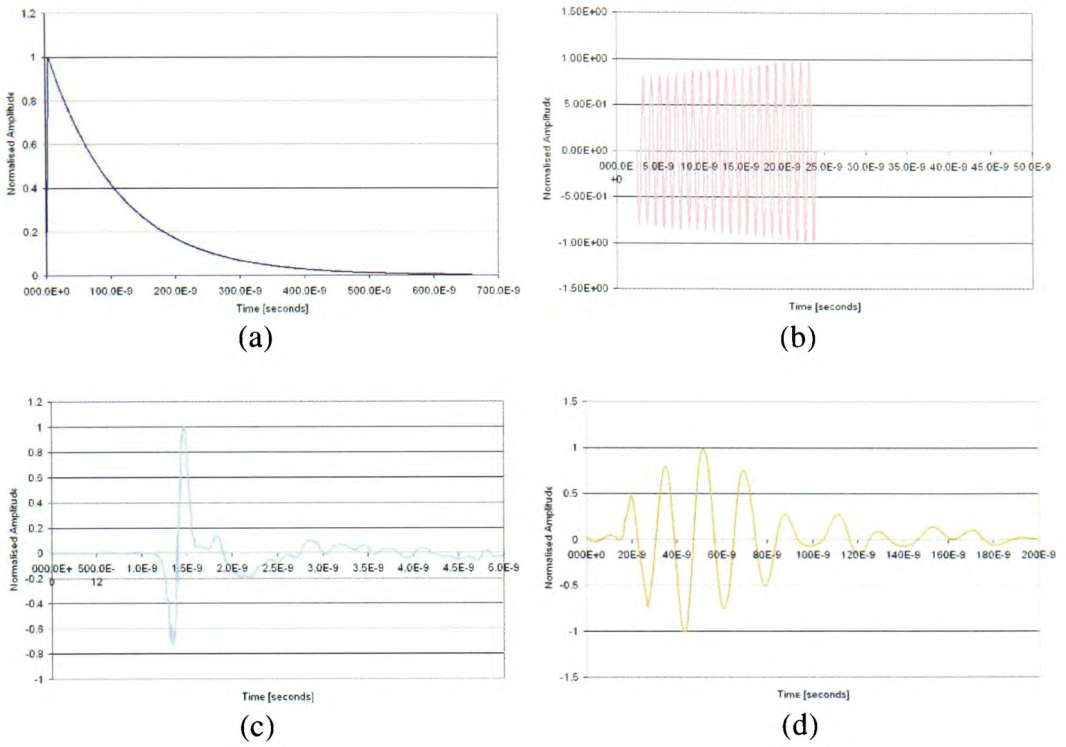


Figure 11: Time domain representation of each waveform type:
(a) Simulated EMP ($t_r \approx$ 10ns, Full width half maximum (FWHM) $\approx$ 150ns);
(b) Simulated Hypoband (f $\approx$ 1GHz, pulse width $\approx$ 25ns) ;
(c) Hyperband ($t_r \approx$ 100ps)
(d) Mesoband (Centre frequency $\approx$ 50MHz)

EMP is generally considered to comprise of a single pulse event but it is possible to have many pulses per second for Hypo, Hyper and Mesoband waveforms. This is known as repetition rating, the interval or more precisely the frequency of pulses is known as the pulse repetition frequency (p.r.f). Figure 12 demonstrates the effect of repetitive pulses of a Hypoband waveform in the time domain.

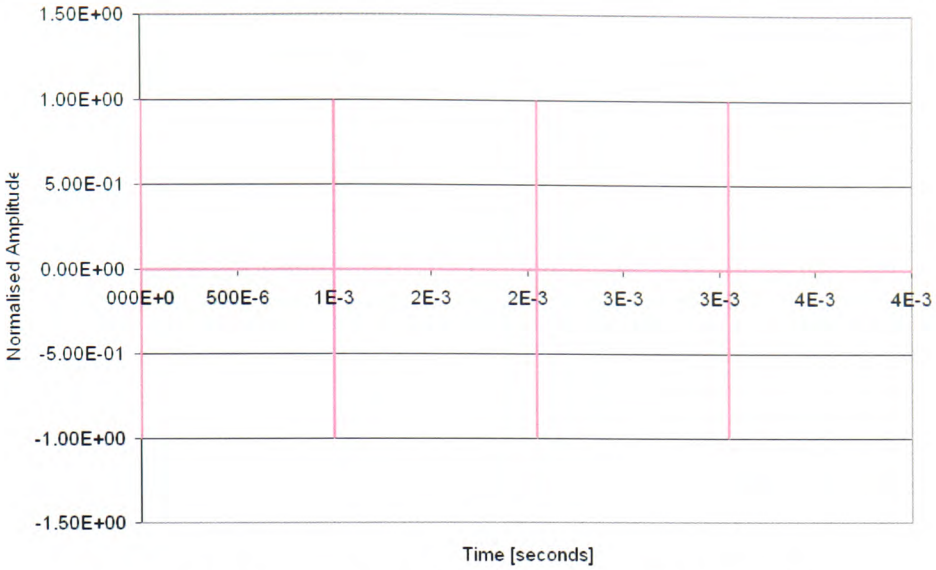


Figure 12: Repetition rated Hypoband waveform (p.r.f ≈ 1kHz)

The time domain features of the waveform type have a large bearing upon the efficiency of the EM interaction. This is discussed in some detail in Appendix A, Section 6.6.

Figure 13 shows the pulse frequency spectra for the different EM disruptor waveform classes in the frequency domain.

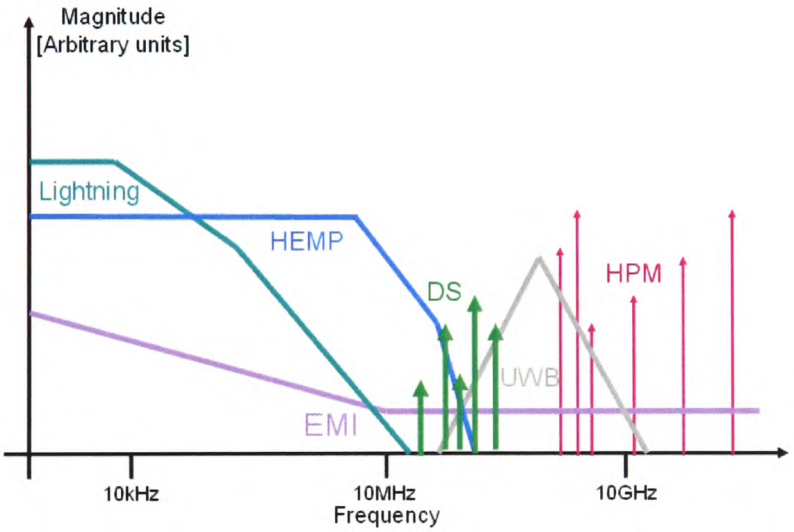


Figure 13: Frequency spectra of disruptor waveforms (Adapted from IEC 61000-2-13)

2.3.3 Principles of the method

Referring to the model from of Figure 3, a typical schematic diagram of the concept is given in Figure 14.

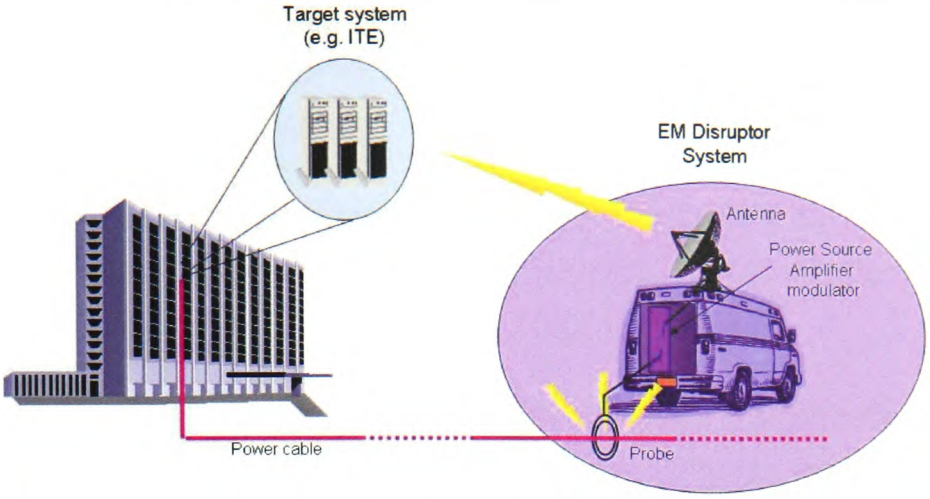


Figure 14: The EM disruptor threat concept

In this diagram a vehicle containing the necessary prime power and amplification/modulation equipment is used to generate high level EMI which can be used to stress and potentially disrupt or damage information processing systems housed within an installation by radiated or conducted means.

2.3.3.1 The Victim

The victim of EM disruption can be any form of electrical or electronic system. Unlike the EM interceptor threat it may not be necessary to precisely target information processing systems since secondary or cascade effects may be possible. For example consider that an EM disruptor could be used to activate an electronic fire alarm control unit to allow a thief to gain entry or perhaps activate sprinkler systems in a central processing facility causing flood damage to information processing systems.

In general the elements which could be subjected to an EM disruptive threat can be considered in a hierarchical sense based on their specific geometry and dimensions this is discussed in Appendix A, Section 6.1.

2.3.3.2 Disruption Mechanisms

The actual process of inducing disruption in an electronic system, the disruption mechanism, is complex and the subject of much research [UIC, 2001], [UNM, 2001].

In order for an electronic system to be affected by an EM disruptive waveform it must clearly capture some energy from the waveform. This process is known as coupling and was discussed in relation to Figure 3 earlier and in more detail in Appendix A, Section 6.5.

In general the coupling efficiency (i.e. the amount of energy absorbed into a system) is increased when the wavelength of the impinging RF field is comparable with the dimensions of the coupling structure.

For infrastructures (cable lengths greater than a few km) the waveforms with the highest coupling efficiency are those with frequency content (in the tens of kHz) possessing wavelengths proportional to cable lengths such as HEMP and LEMP.

For an installation (e.g. an office building containing a computer network) the stress can couple through apertures such as windows and doors or through conductive utilities which penetrate the installation.

For a computer network the most likely coupling route is via the interconnecting cables such as network or power cables (cable lengths up to a few 10's of metres). The optimum waveform for coupling will have higher frequency content (a few MHz) than HEMP and LEMP, therefore VHF Mesoband waveforms are likely to be most effective.

At the system level (dimensions less than a few metres) the interaction is predominantly either aperture or cable coupling. The apertures on a system generally have a smaller area than the cable loops. It is therefore expected that microwave Hypoband and Hyperband type waveforms (frequency content greater than 1 GHz) will couple well to cables and apertures of small systems such as computer systems. The EM stress then penetrates inside the system to circuit boards and further to the sensitive electronic components.

The examples above are all representative of back door coupling to the system i.e. through unintentional antennas or apertures. Front door coupling through intentional communications and non-communications (such as radar) ports is also possible and was discussed in the context of EW in Section 2.1.4.1. Systems, networks, and even infrastructures can have antenna ports. The risk of damage to components at the base of the antenna port (i.e. the receiver) may be high because there is a direct conduit for the EM stress especially if the disruptor waveform frequency spectra are within the bandwidth of the antenna port. Even harmonics of the EM disruptor waveform have the potential to be highly stressing to the parasitic elements of a receiver.

For back door coupling the actual mechanism in which the EM energy interacts with a circuit or system and causes upset is also very complex [Gaudet, 2004]. The most popular theories are based on:

- Rectification of non linear elements on the circuit which can be actual component junctions or parasitic elements
- Intermodulation whereby several non linear structures create a beat frequency in the pass band of the device [Chase, 1975]
- Altering logic levels by generating offsets
- Altering logic states by introducing glitches
- Changing power supply conditions
- Introduction of chaotic behaviour [Andreadis, 2004]
- Damaging the semiconductor junctions by the avalanche effect or power supply follow through, or other thermal effects [Camp, 2002]
- Any combination of the above

At the circuit level therefore, the level of upset is dependent on the circuit operating voltage level (power supply), the logic or switching level, the operating frequency range of the devices (clock speed and bandwidth) and the number and type of potentially rectifying elements (i.e. component density).

The trend for semiconductor technology is moving towards lowering the supply requirements and switching logic levels and increasing the operating frequency and component density on the chip [ITRS, 2005]. Some graphs showing the predicted trends adapted from the International Technology Roadmap for Semiconductors (ITRS) are shown in Figure 15 and Figure 16.

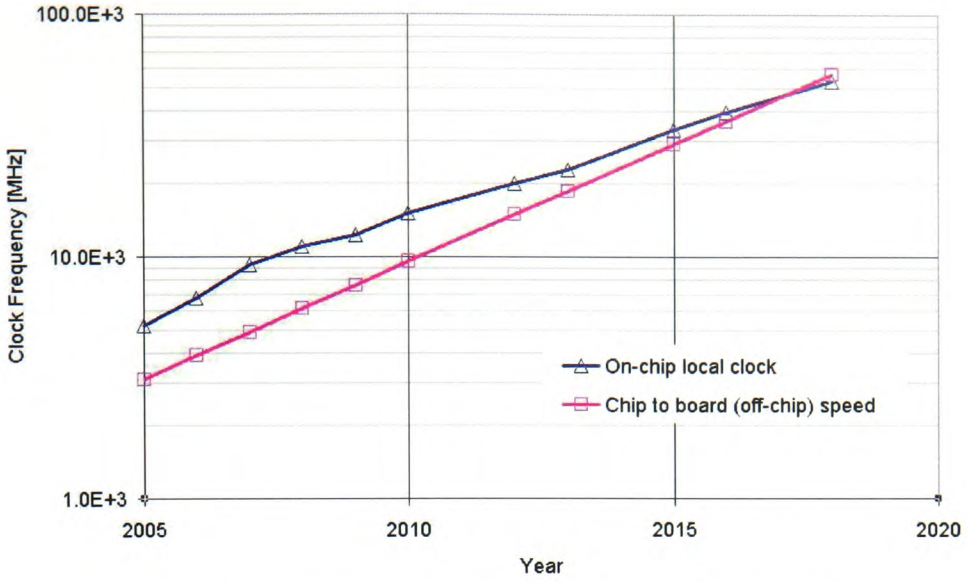


Figure 15: Predicted trend in clock speed for devices and circuits

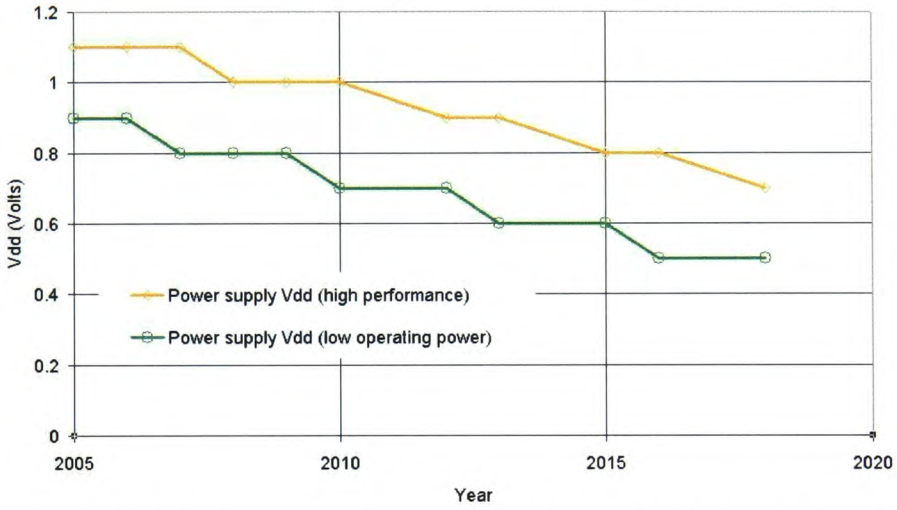


Figure 16: Predicted trend in Power supply requirements for devices and circuits

These trends have prompted some [Baffreau, 2002], [Kohlberg, 2002], [Armstrong, 2001] to predict that systems will become more susceptible to interference and disruption in the future.

In general it is very difficult to predict the coupling and disruption mechanisms of the victim. This is because of the large uncertainty, number of variables or degrees of freedom related to the EM interaction. It is not presently considered possible or practical to predict with any degree of certainty the EM coupling, propagation mechanism, and circuit response of a complex victim system. Some reasons for this complexity are discussed in Appendix A and other uncertainties are provided in IEC 61000-1-5. These are listed below:

1. The status of the system logic state and pending operations at the time of EM illumination

2. The coupling efficiency of the stress into the system, due to the large number of important parameters, whose values are unknown or variable

3. The unknown or time-varying orientation and distance of the system with respect to the EM source

4. Variations in the system susceptibility level for nominally identical systems

Another potential source of uncertainty for disruption at system level is that commercial standard systems supplied by the same manufacturer and from the same assembly line may look identical from the outside but have very different devices on the circuit boards within.

2.3.3.2.1 Upset and Damage

Two broad classes of induced effect from EM disruption are possible for the victim system, upset or damage, although in a functional context there are many shades in between. Upset is sometimes referred to as soft kill and damage as hard kill.

For the examples in the introduction the effect of the disruption from the Starfish EMP event was loss of power to houses caused by damage to the power transmission system. Whereas, the effect of EM disruption on Forrestal was damage to materiel and the deaths of servicemen caused by EM induced upset of missile launch electronics.

Consider the trivial example of a notebook computer as a target for the EM disruptor. When the notebook is exposed to EM stress the user may experience a range of induced effects such as; mouse or keyboard malfunction (irregular mouse movement, false keystrokes); hard disk latch up; through to switch off or shutdown. Further, on investigation the user may find corrupted data, or even damage which may have rendered the notebook unusable.

However, there is another dimension to the effect concerning the impact on the system function. If the notebook was being used to surf the internet then mouse deflection may only be an inconvenience to the user of the notebook. But if the same effect was experienced when the notebook was being used for some critical function (i.e. manoeuvring a robot arm on a vehicle production line) then the consequence could be

greater. For example mouse deflection could cause the arm to smash into the vehicle potentially damaging the robot and costly downtime for the production process.

In general more EM stress is required to produce damage than that required to initiate upsets. A six point scale has been proposed to quantify disruptor effects [Ross, 2004]. This scale is given in Table 2.

Level	Effect	Impact
0	No immediately observable effect	Victim functions are normal
1	Effects present during illumination by disruptor	Effects observed but do not require corrective action
2	Soft reset – operator intervention required	No need to cycle power on/off
3	Hard reset – operator intervention required	Need to cycle power on/off, limited downtime dependent on system function
4	Maintenance action required, temporary fault	Technician required to fix fault, increased system downtime
5	Physical damage	System inoperable / replacement required

Table 2: Disruptor effect scaling

In summary then the effects induced in a system exposed to EM disruption are complex. The induced effect on a system is at least dependent upon:

- Victim system type
- Victim system function
- 'Stressing' features of the disruptive waveform
  - Frequency
  - Bandwidth
  - Coupling Efficiency
  - Magnitude
  - Rate of Rise
  - Energy

For deployed EM disruptor systems in 'real world' scenarios other factors such as the propagation or path loss, structural attenuation and illumination volume are also very important factors which add to the complexity of the issue (see Appendix A).

2.3.3.3 The EM Disruptor Source

The essential elements of an EM disruptor source can be simplified to the list below:

- Access to some form of prime power
- An energy storage mechanism
- A modulator - to develop the EM waveform
- An antenna - to radiate the high power EM waveform or a transducer to inject a high voltage or high current RF waveform into a conductor

There are a large variety of components which can be used in many different ways in order to achieve an EM disruptor system design. The main goal for all of these systems is to achieve very high peak or average power (stress) which is subsequently delivered to the victim system. It is important to recognise and discuss these variations in order to develop analytical expressions and as a tool to develop further discussion. It is also important to realise that the technical capability of the disruptor designer and the scenario for which the disruptor will be deployed will affect the choice of component.

2.3.3.4 Technical Capability/Scenario

The technical capability can be considered at two extremes. The lowest capability group will be referred to as 'Low Tech' where this applies to a well funded amateur, hobbyist or hacker with access to commercially available components and some workshop space. The highest capability group will be termed 'State of the art' where this refers to National Government (usually military) research departments with all available resources and state of the art facilities. It is expected that other adversaries such as criminals, terrorists, and NSA's will have a capability somewhere between these extremes.

For a Low Tech EM disruption source commercial availability of components, cost, and technical skill will influence the design. For a State of the art EM disruption source it can be assumed that the EM disruptor simulator systems built by government research agencies and discussed in the open literature (at conferences etc.) are likely to be representative of the state of the art.

Schriner [Schriner, 1998], postulates three different scenarios for improvised or Low Tech disruptors whereas for military use other scenarios have been considered [Stark, 2004]. A condensed set of scenarios for deployment of disruptors can be considered to be:

1. Man portable systems – for close 'hand en-placed' deployment (i.e. an EM disruptor which can be taken inside an installation and which can therefore expose a system unimpeded)

2. Mobile systems – for example housed within a van or tracked vehicle (i.e. similar in principle to the concept shown in Figure 14 which have to overcome range limitations and the attenuation of the installation structure (see Appendix A)

3. Fixed installations – in military parlance these could be large platform i.e. ship based, or fixed land based stations for suppression of enemy air defence

4. Deliverable non re-usable disruptor systems – such as RFM where the disruptor is delivered to the target/victim and destroyed in the process

These scenarios undoubtedly affect the choice of components for the disruptor designer since parameters such as size, weight, concealment, power requirements, etc. will have an impact on the overall disruptor design. The choice and availability of components will in turn affect the likely range and effectiveness of the disruptor.

2.3.3.5 EM Disruptor Source elements

2.3.3.5.1 Prime Power and Energy Storage

This could be the domestic power (mains) supply, batteries, portable or fixed generators, explosives or any other means[6] of generating the electrical energy required to eventually radiate from the antenna. The type of prime power deployed is obviously dependent on the scenario in which the disruptor will be used, the average power requirement of the modulator and the overall efficiency of the system.

For man portable disruptors some form of portable power must be used if access to the domestic supply is not possible. Batteries are the most likely prime power component for

the man portable scenario. Batteries can also be considered as energy storage devices but in many cases it may be necessary to have a storage stage.

For mobile systems it may be possible to use the vehicle electrical system to provide prime power for longer (if the engine is running and trickle charging the system). Alternatively a portable petrol or diesel generator could be used.

For fixed installations the domestic or even an industrial electrical supply could be accessed to provide the prime power requirements for the source.

Typically capacitors or inductors or some combination of these components such as a Blumlein or Pulse Forming Networks (PFN) or Pulse Forming Lines (PFL) [Martin, 1996] may be used to shape the energy for delivery to the modulator.

2.3.3.5.2 Modulator

The term modulator is used here to represent the key component or group of components, which convert the steady state prime power to an EM waveform capable of being radiated by the antenna.

The simplest form of modulator is a high power switch which effectively 'dumps' the electrical energy from the energy store into the antenna. Other forms of modulator can include relativistic tubes (Gyrotrons, Klystrons, Reltrons, Vircators and in particular Magnetrons), Marx generators, Tesla transformers and complex solid state systems. The number and variation of modulator types is large, a brief summary is provided here:

For Low Tech modulator designs high power tube technologies which are used for RF broadcast or radar applications are readily available for public sale. Tubes like the Eimac 8974/X-2159, which is capable of producing 2 MW peak power in the low VHF band (30 MHz) [Eimac, 2005] and the Burle 4664 tube capable of producing 3 MW at 540 MHz with a 3 % duty factor [Burle, 2005] would be available to the amateur/hacker. However, the level of technical sophistication required of the engineer to incorporate these tubes into a working system is likely to be high. Very high power Klystron modulators up to 50 MW are available for very specialist applications such as the Compact Linear Collider (CLIC) at CERN [Pearce, 2000].

[6] For many EM disruptor system types these prime power and energy storage elements may be combined, for example an RFM may use explosive (chemical energy) to provide prime power, store energy and even effectively modulate the EM signal.

The modulator in a typical microwave Hypoband system will probably be based on conventional or relativistic tube technology **0**Benford and Swegle, 1992]. Example HPM modulator types include, Travelling Wave Tube (TWT) amplifiers, Magnetrons, Backward Wave Oscillators (BWO), Magnetically Insulated Line Oscillators (MILO), Gyrotrons, Klystrons, Reltrons, and Vircators. The limitation with tube oscillators is that they are resonant cavities i.e. their dimensions and structure only allow modulation to occur over a narrow range of frequencies. Of the tube types above the Magnetron is perhaps the most common and most well known since it is the principal component in domestic microwave ovens. Indeed Low Tech microwave Hypoband disruptors have been manufactured using microwave oven magnetrons or even ex-military radar magnetrons. The Vircator however is considered to be the most versatile microwave Hypoband modulator type since it is able to be tuned to several different frequencies within a narrow range (up to ≈ 10% of the centre frequency) [Benford, 2004].

A photograph of a high power relativistic magnetron is given in Figure 17.

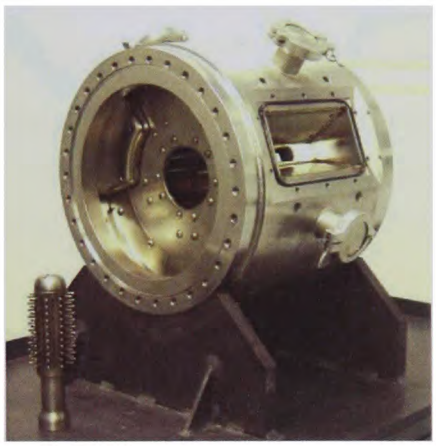


Figure 17: High Power magnetron and pin cathode

Microwave Hypoband modulators can be engineered to produce repetitive pulses, however, due to the large average power requirements and general inefficiency of the process (≈ 20 % to 30 %) the repetition frequency is generally limited to a few hundred Hertz at most. The pulse duration is dependent on the prime power availability and the tube type. Pulse widths of a few hundred nanoseconds are achieved with very high peak power tubes (1 GW), wider pulse widths (a few tens of micro seconds) are available with lower peak power systems. Microwave oven magnetrons, work with a 50 % duty cycle (i.e. the energy is 'on' half of the time), but the peak output power is limited to about 1 kW.

A typical VHF Mesoband system can be implemented using very similar technology to that required to simulate HEMP waveforms. The most common configuration is a Marx generator with an oil or gas spark gap switch at the output which discharges the stored energy in the Marx into an antenna [Kekez, 1989]. A Marx generator is a parallel charged *n* element resistor/capacitor energy storage system, the parallel elements are connected in series to effectively sum the energy in the parallel stages. By adjusting the configuration of the spark gap it is possible to change parameters such as rise and fall time which affect the bandwidth of the signal produced. However, the oscillating frequency of the radiated waveform is primarily a function of the antenna geometry. A limitation of spark gaps is that the repetition rate is limited by the physics of the breakdown process within the spark gap. The highest repetition frequency presently achievable is 5 kHz [MacGregor, 1997].

Hyperband modulators can also employ Marx generators. Other modulator types can include Tesla transformer or solid state switches can be used. A Tesla transformer is a high-voltage, air-core, self-regenerative resonant transformer that generates very high voltages at high frequency. Solid state technology such as Integrated Gate Bipolar Transistors (IGBT), Drift Step Recovery Diodes and Transistors (DRSD and DRST), Stacked avalanche switches, Silicon Avalanche Shapers (SAS), Semiconductor opening switches (SOS) and Photo Conducting Solid State Switches (PCSS) are discrete silicon components which can be employed in arrays and circuits to develop the UWB waveform [Richardson, 2000], [Kardo-Sysoev, 2000], [Agee, 1998]. The unique requirement for Hyperband modulators is the need to generate very fast rise time pulses, since the rise time of the pulse is directly related to the highest frequency in the pulse frequency spectra. Many Hyperband systems employ some form of pulse sharpening, such as fast spark gap switches or ferrite loaded shock-lines [Brooker, 1999] to improve the rise time of the pulse. A limitation of the Marx variants of UWB modulators is that they rely on spark gap switching which limits the highest repetition frequency achievable. Solid state systems can have repetition frequencies up to 600 kHz. Low Tech Hyperband modulators have been developed using Tesla or other step-up transformers.

The combination of a prime power source, an energy storage device and a modulator is known as a pulsed power system.

2.3.3.5.3 Antennas

Some properties of antennas are discussed in detail in Appendix A, Section 6.4. In most practical cases the basic requirements for EM disruptor antennas are:

a) To efficiently convert the EM modulated waveform to a radiated waveform

b) To deliver the maximum stress to the victim which implies that the antenna must have gain or directivity

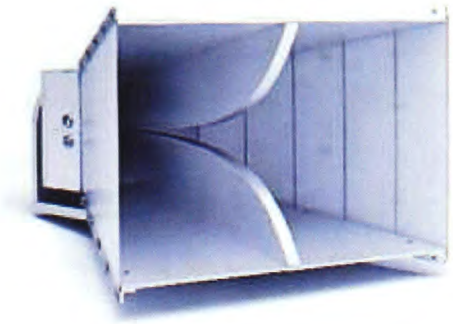
c) To faithfully radiate the waveform characteristics, such as rise time, pulse width etc. or to enhance or create modulation of the waveform through radiation

d) Not to generate a voltage gradient which exceeds the air dielectric breakdown (nominally 3 MV/m)

e) To be able to handle the power output of the modulator

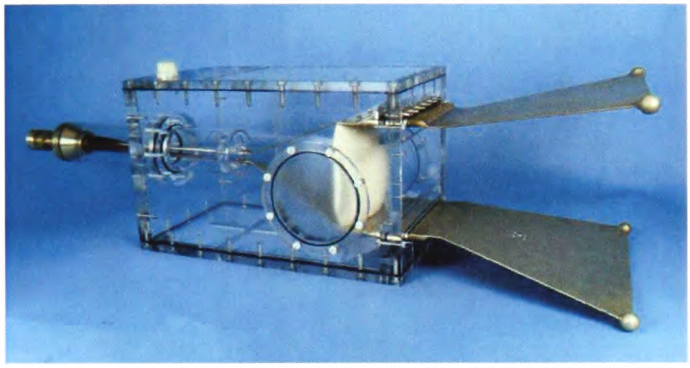
f) To have an input feed which is impedance and geometry matched the output feed of the modulator

The antenna gain or directivity (discussed in more detail in Appendix A, Section 6.4) ensures that the majority of the stress generated by the disruptor is delivered to the victim system, enhancing the stress at the victim and therefore maximising the probability of disruption. Antennas with poor directivity such as dipoles and monopoles are not ideal since the energy is radiated in all directions in the plane of the antenna. However, highly directive antennas (gain 30dBi to 40dBi) are usually large especially at frequencies up to a few GHz. Large antennas are difficult to conceal and portability would be an issue for the man portable scenario. Some photographs of typical antenna geometries are given in Figure 18.

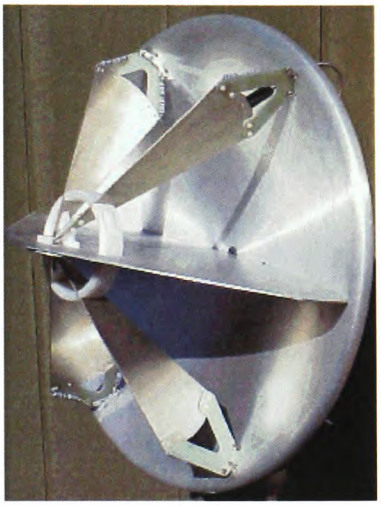


(a)

(b)



(c)



(d)

Figure 18: Some examples of different disruptor antenna types
(a) Standard Waveguide horn
(b) 2.4m offset horn fed parabolic reflector
(c) Co-axial fed Hyperband TEM horn with dielectric lens
(d) Hyperband IRA

In the microwave frequency region (above 500MHz) the most practical form of antenna used is the waveguide horn or an array of horns [Rahamat-Samii, 1992]. The waveguide horn has good efficiency and directivity and the input to the antenna is usually a waveguide structure which matches the output of the microwave modulator. It is also feasible to construct rudimentary waveguide horns with Low Tech means.

The horn may be filled with a dielectric material for very high peak power sources where the electric field stress at the antenna feed point may exceed the breakdown of air or have a dielectric lens to shape the wave front. For frequencies above a few GHz a dish reflector may be used together with a feed horn in order to achieve greater gain or directivity. At frequencies below 1GHz the size of the horn becomes large and other

antenna schemes such as log periodic or array antennas can be used to provide directivity.

For Hyperband waveforms the antenna must be broad band and capable of handling very high peak voltages. The preferred antenna types are the Transverse Electromagnetic Mode (TEM) horn [Holzman, 2000] or the Impulse Radiating Antenna (IRA) [Farr, 1999]. A TEM horn is simply an open ended parallel plate waveguide with flared plates at the end which act as an impedance gradient to attempt to match the modulator output impedance to air. An IRA consists of a parabolic reflector with a TEM feed. Very good directivity is possible from an IRA.

2.3.3.5.4 Transducers

According to the earlier model (Figure 3) there is also the possibility of using conducted rather than radiated means of disruption. In this case the antenna is replaced with a suitable probe which can inject high voltage or high current RF pulses onto power, telecommunication or signal cables, or indeed other conductors.

In most practical cases the basic requirements for EM disruptor transducers are in many ways similar to the requirements for antennas, some difference are highlighted below:

a) To efficiently convert the EM modulated waveform to a conducted current or voltage

b) To faithfully reproduce the waveform characteristics, such as rise time, pulse width etc. in the victim system conductors

c) Not to generate a voltage gradient which exceeds the dielectric breakdown of the conductor of the surrounding dielectrics such as the soil

Three main injection mechanisms can be considered:

Point injection – i.e. a suitable probe is brought into direct contact with the victim conducting channel

Capacitive coupling – e.g. an electrostatic charge is built up on a plate or similar structure and induces an opposing charge in the victim conducting channel

Magnetic induction - This could either be a 'lossy' cable laid along in parallel with the victim conducting channel or a current injection probe or transformer which is placed

around the victim conducting channel where the latter forms the secondary of the transformer.

2.3.4 Complete EM Disruptor Systems

Complete EM disruptor systems employing all of the elements, prime power, energy storage, modulator, and antenna/transducer have been discussed in the open literature. For example Orion is a state of the art UK based microwave Hypoband simulator operated by QinetiQ. An annotated photograph of this simulator is given in Figure 19.

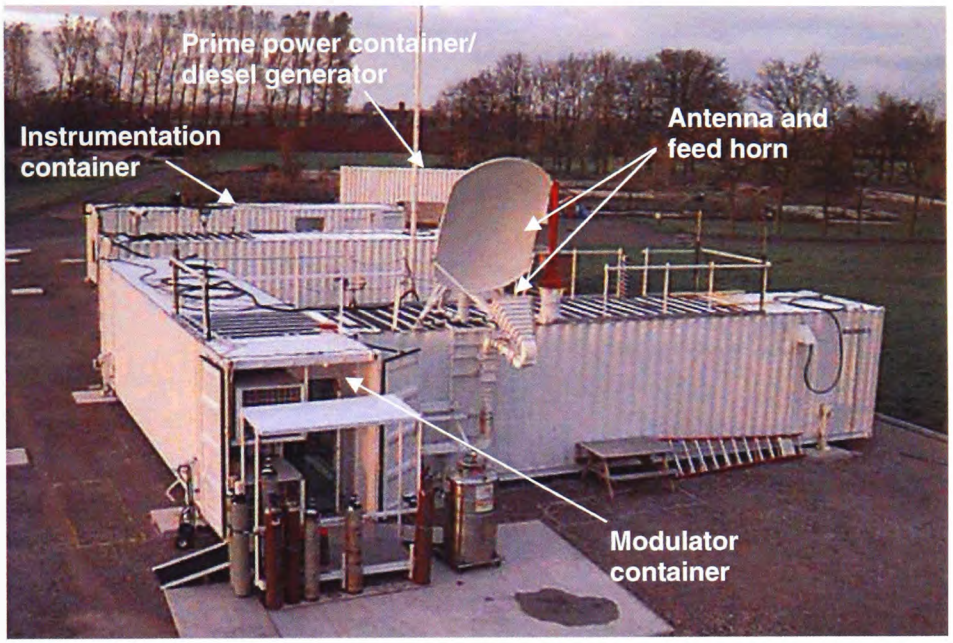


Figure 19: The Orion Hypoband simulator

2.3.4.1 Low Tech - Radiated Disruptor Systems

Plans, descriptions and demonstrations of Low Tech disruptor systems are available on the Internet. The systems discussed in these open forums range from HPM, and UWB like systems through to RFM like systems. A short summary of some of the web sties is provided in Table 3.

Site URL	Description
http://strike-free.info/ready.gov_ebomb.htm	Contains diagrams of how to construct an E-bomb
www.plans-kits.com/plans/plans.html	Sells plans and kits of crude but potentially high power RF sources, including access to 'Microwave EMP (long range weapon) research papers' for $25. The site also offers military specification magnetrons.
http://www.ttr.com/	Tesla Technology Research site, claims to be the world's leading manufacturer of Tesla Coils. The site has information on designing and building Tesla Coils and guides on purchasing a Tesla Coil system, component assembly, and individual parts. Also contains links to other Tesla related sites.
http://www.voltsamps.com/	Shows how to design HERF weapons from microwave oven magnetrons and also has videos of the design and effects on a computer victim. The site mentions other effects on fluorescent tubes and motion detectors. Pictures and discussion of the David Schriener source which was demonstrated at Infowarcon are included. Since visiting the site in February 2004, the site has been removed by the author (September 2004)
http://www.power-labs.com/emguns.htm	Designs of an Electromagnetic gun (microwave oven magnetron based) amongst other weapon concepts such as rail guns and laser weapons
http://www.eio.com/public/inductor/0024.html	Describes how to build three types of HERF or EMP 'guns'. These are an omnidirectional RF burst device, an RF gun, and a microwave gun.
http://www.amazing1.com/emp.htm	Two designs of EMP/Shock generators, plans available for $20, or a 1.8GW version available to rent at $1500 per month or buy for $7495. Appears to be based on arc welder type technology with a simplistic reflector antenna

Table 3: Complete Low Tech disruptor systems

A quick review of the designs offered above shows that they are unsophisticated and rudimentary using well known voltage multiplication circuits or concepts borrowed from other high voltage generation systems (such as car ignition systems). Some if not all of the designs could result in personal injury to an amateur/hacker designer during manufacture let alone during operation.

The Low Tech microwave Hypoband like disruptors are mostly based around a 1kW Microwave oven magnetron with a home-built waveguide horn. The microwave oven magnetron requires a few hundred Watts prime power and therefore must be mains power driven. This source could feasibly be deployed in the man portable scenario if mains power was readily available near to the victim system. A battery and inverter could be used but the burst time would be significantly limited.

The Schriner TED system was the subject of a US military 'Live Fire Test' of RF weapons at the Naval Air Warfare Centre Weapons Division (NAWCWD), Valley

junction test range, China Lake [Henderson, 1998]. The TED system was manufactured from commercially available components based on an automotive ignition system and an oil cooled spark gap switch which appears to have been the primary output switch. The radiating antenna structure was a home made TEM horn. Although not explicitly discussed in relation to the Schriner TED source rise times of 100 ps, with E-field 20 kV/m at 10 m and a 1 kHz pulse repetition frequency are discussed in the Henderson article.

For a well motivated and well funded amateur complete fixed and mobile ex-military RF broadcast and search radar systems are available on the internet. One site offers a complete 1.3 GHz 2MW search radar (AN-FPS-71) which would require a fixed installation and a compete mobile 1.2 to 1.3 GHz 500 kW system [RRIC, 2004].

2.3.4.2 State of the art - Radiated Disruptor Systems

The state of the art the systems which are described in the open literature are not disruptors but are used to simulate high power RF environments for susceptibility and EM effects research or for EM hardening and protection research or even for HIRF clearance of civil and military aircraft. This research is invariably conducted by National government defence organisations, often in partnership with Universities. Indeed it is clear from the open literature that countries such as Canada, China, France, FSU, Germany, Sweden, US, and UK operate high power disruptor simulator systems. Two very useful references have been found which summarise state of the art world-wide DS, UWB, and HPM activities [Sabath, 2004].

2.3.4.2.1 RFM

For RFM the goal is convert chemical or explosive energy into radio frequency energy. The most widely discussed mechanism to achieve this is the MCG which can be use to drive a switch or antenna directly or alternatively to drive a HPM tube such as Vircator or MILO [Novac, 1998]. The MCG (and variants such as Helical FCG, MCG, and MHD) is essentially an explosively driven variable inductor. The inductor is wound on an explosive former, and electrical energy is stored in the inductor. When the explosive charge is activated the inductor diameter expands which compresses the magnetic flux in the inductor causing magnification of the energy. RFM systems are effectively 'one-shot' disruptor systems although it is possible to conceive that multiple devices could be used together producing a larger overall stress or a pseudo repetition frequency.

Although there is much speculation about individual component parts of complete RFM systems, schematic diagrams of complete systems, and quoted peak power outputs (≈ 1 GW) very few references to actual deployable systems could be found in the open literature.

2.3.4.2.2 HEMP Simulators

HEMP simulators simulate over a small volume one of the waveform components which is generated by a high altitude nuclear explosion. HEMP simulators used non nuclear means to generate this waveform and are primarily used to validate the hardening and protection of military equipment to the HEMP environment. In most cases these simulators are driven by a Marx generator which feeds a PFN or PFL through a spark gap switch to the antenna. Generally the antenna is formed into a bounded wave or parallel strip line construction [IEC 61000-4-32, 2002]. In this way the electric field is predominantly contained within the bounds of the simulator and not freely radiated. Examples of HEMP simulators are the TRESTLE simulator shown in Figure 10 and the QinetiQ HEMP simulator.

The QinetiQ HEMP simulator is housed within a separate wooden building designed specifically for the minimisation of RF reflections. The simulator consists of a Marx generator, PFN and bounded wave antenna. The working volume is 4m wide by 4m deep by 4m high and the field has good uniformity within this region.

The IEC 61000-4-32 document titled 'EMP Simulator compendium' has specifications for over 39 simulators from over 13 countries around the world.

2.3.4.2.3 Hyperband Simulators

An example of a state of the art Hyperband disruptor simulator is the JOLT system discussed by Baum amongst others [Baum, 2004]. JOLT is a large UWB simulator which appears to have been developed for a mobile scenario although the prime power requirements are not discussed. The simulator comprises of a rectangular capacitor energy storage section, a 22:1 step-up pulse (Tesla) transformer which up converts the 50 kV stored in the capacitors to 1.1 MV, a compact gas filled spark gap switch to transfer the transformer output to a peaking section and peaking switch (an oil filled spark gap). The antenna employed is a Half-IRA with a TEM feed. The JOLT source is capable of producing a 150 ps rise-time impulse with a pulse width of approximately 400 ps, providing an approximately flat spectrum from 500 MHz to 2 GHz. The measured peak

E-field is 80 kV/m at 85 m. The maximum achievable repetition frequency appears to be 600 Hz, burst limited to one thousand pulses. The source appears to be burst limited to a few seconds because of prime power constraints.

Other examples of Hyperband systems are the Radan compact modulator from the Russian Academy of Sciences in Ekaterinburg, Russia. This modulator utilises solid state switches and gas filled spark gaps to deliver 180 kV with a 150 ps rise time, a 1 ns pulse width at a maximum repetition frequency of up to 1 kHz. The modulator is 'desk-top' size and has a co-axial output which can be used to feed conventional antennas. Due to the compact nature of the source it may be possible that this source is capable of performing in the 'mobile' scenario.

A very compact, very high repetition rate UWB system is the HRR32 manufactured by Diehl Muntionssystem. The prime power is provided via batteries which fit within the packaging dimensions but this limits the operating system time to 20 minutes. Alternatively a mains powered 24 volt power supply can be used allowing the system to run continuously but this limits portability. An inverter supply of some sort must be incorporated but specifications are not provided; this is likely to be solid state. The system uses 32 parallel spark gaps each running at a very high repetition rate. This produces a random p.r.f. with a maximum measured p.r.f. of 1 MHz, and an average of 600 kHz. The HRR32 uses monopole antennas (which also act as a tripod stand for the system) to radiate the UWB waveform.

Other compact solid state UWB modulators are manufactured by Bournelea and Kentech in the UK, FID GmbH and Diehl Muntionssystem of Germany, and Diascarb Research in Kiev, Russia.

2.3.4.2.4 Microwave Hypoband Simulators

The prime power source for the UK Orion Hypoband simulator consists of two, three phase 100 kW electrical generators and a 500 kW diesel generator. The 100kW generator drives the charging system PFN where the output of the generator is converted to a 30 kV DC supply. This supply is then coupled into the power modulator where the DC voltage is stepped up to 1 MV. The primary modulator is a magnetron. In the magnetron approximately 10% to 20% of the electrical power is converted to RF power resulting in ~300 MW of microwave power extracted from the magnetron. The antenna consists of a waveguide feed horn and an offset fed parabolic reflector. The antenna is designed to provide 26.7dB of gain over the Orion operating frequency range. The complete

specification for the Orion source is given in Table 4 [Kerr, 2004]. This highlights some of the logistical and infrastructure requirements for state of the art EM disruptor systems.

Parameter	Specification	Comments
Tuneable Bandwidth	1.0 to 3.3 GHz	
Output Power	> 300MW	This is the minimum across the entire operating bandwidth.
Field at target	>30kV/m	This number is specified as a minimum across the target area at 75m range.
Target area	7m x 15m	Ensures full illumination of large targets.
HPM Pulse Duration	50 to 150ns @ >200MW <500ns @ <50MW	This is limited by the magnetrons not the pulsed power supply.
PRF	Single shot to 100Hz	Few HPM system can achieve >10Hz.
Time between bursts	8 minutes	Determined by thermal relaxation.
Cool down time	approximately 1 week	Cooling the magnets down from room temperature is a multi-stage process.
Magnetron changeover	2 Days	This time allows for reconfiguration of all relevant software and hardware.
Cathode changeover	1 Day	
Morning Start-up time	1 hour	All systems must be booted and diagnosed for problems.
Evening shut-down	½ hour	Series of simple shut down procedures.
Magnet Helium hold time	3 days	The magnets have to be refilled with Helium every three days.
Helium consumption	250lts/week	expected
Frequency change	2 hours	Time is required to retune and optimise the system.
Magnetron A Bandwidth: B C D	1.07 1.31 1.32 1.80 1.81 2.30 2.31 3.3	To move between each magnetron operating frequency requires a two day turn around.
Power supply Impedance	50Ω	This matches with the impedance of the magnetrons.
Electrical Pulse Duration	150ns to 500ns	In 50ns steps.

Table 4: Complete specification for the Orion HPM simulator

This detailed specification with the inherent restrictions on operation is typical for many of the state of the art Hypoband systems.

The Microwave Test Facility (MTF) is a Swedish Hypoband simulator which is used for HIRF certification of military aircraft. The MTF is installed in a 12 m container and has a separate prime power unit which is an AC diesel generator. The system consists of five separate klystron type microwave tubes, with centre frequencies of 1.3 GHz, 2.86 GHz, 5.71 GHz, 9.3 GHz and 15 GHz. The maximum pulse width of the output pulse is 4.5 μs, with a maximum pulse repetition frequency of 300Hz. Repetition frequencies of up to 1kHz are possible whilst keeping within the average power constraints of the system. The antenna used is a waveguide horn or alternatively a special type of high gain reflector antenna (Cassegrain) can be used for the 2.86 GHz and 5.71 GHz frequencies. At 1.3 GHz the peak E-field is quoted as 30 kV/m at 15 m. At 2.86 GHz, using a special pulse compression system, up to 80 kV/m at 15 m is quoted. The maximum burst length is limited to 10 seconds.

The German Hypoband simulator known as Supra utilises a thyratron switched PFN-Marx which drives a Super-Reltron microwave modulator. Four Super-Reltron tubes cover the frequency range 0.675 to 1.44 GHz although it is planned to add four other Super-Reltron tubes to increase the maximum frequency to 3 GHz. The maximum pulse width is 300 ns with a maximum p.r.f. of 10 Hz. The system is limited to 100 pulses per burst. Specially designed dielectric filled waveguide horns are used to radiate the HPM signal into an anechoic chamber. The peak E-field is quoted as 70 kV/m at 15 m. Other Hypoband simulators of note which have been discussed in the open literature are:

- The French Hyperion system [Sabath, 2004]
- The Chinese 1.1GHz, 100Hz p.r.f. Backward Wave Oscillator with a centre frequency of 9GHz [Changhua, 2002]
- The Russian Rosa and Ranets-E 500MW, 9GHz mobile HPM systems [Guoqi Ni, 2005]
- The Indian Kali-1000 system, which has been used to drive a Vircator at 3 to 7GHz [Rao, 2002]

2.3.4.2.5 VHF Mesoband Simulators

A Mesoband system has been described by Kekez [Kekez, 2003]. This system comprises of a DC power supply, compact eight stage 600kV inductor charging Marx modulator with a circular rail spark gap switch in a co-axial geometry. The source produces a 1ns rise time into a matched resistive load. The spark gap geometry appears to be used as the radiating antenna element. The DS source produces the characteristic damped sinusoid or ringing waveform with a duration of approximately 70 ns to 1 μs with centre frequencies of 31 MHz, 86 MHz, 146 MHz and 249 MHz depending on the charging stage configuration used. At a distance of 1.7 m from the source the maximum E-field recorded was 145 kV/m at 31 MHz (70 ns pulse width). The highest pulse repetition frequency appears to be 50 Hz. The system is a laboratory demonstrator which may be capable of being deployed in a mobile or deliverable scenario.

Two other state of art Mesoband sources are the DS110 and DS350 developed by Diehl Muntionssystem in Germany. The DS110 is a compact suitcase sized system which can use batteries for prime power. The source uses solid state technology to develop an input to a very compact Marx generator modulator. The output of the Marx is connected to a

multi-turn cylindrical coil antenna which can be tuned to vary the centre frequency of the radiated waveform. The centre frequency is nominally 375 MHz with at least a 20% bandwidth. The peak field normalised to 1m is quoted as 125 kV/m. This source is clearly applicable to the man-portable scenario.

The DS350 is a larger variant of the DS110 using similar components. The antenna of this source is a multi rod dipole antenna where the length of the rod elements can be varied to change the effective centre frequency of the radiated waveform (nominally 100 MHz). The peak E-field normalised to 1 m is quoted as 300 kV/m and the maximum p.r.f. at the highest output level is 50Hz. The DS350 is specified as a laboratory DS simulator but it is possible to conceive of the source in a fixed or mobile scenario.

2.3.4.3 Radiated Disruptor Systems – Summary

The key parameters of the Low Tech radiated disruptor systems are summarised in Table 5. Parameters for State of the art disruptor simulators are given in Table 6. Some parameters have been calculated / assumed.

Source type	Peak power at antenna (MW)	Maximum Pulse width	Maximum p.r.f (Hz)	Average power at antenna (W)	Antenna type	EIRP peak (W)	Rise time (ps)	Frequency spectrum (operating frequency)	Measured or (Calculated) E-field	$r E_{for}$ [a] (V)	Burst limited? [b]
Low Tech portable HPM (oven)	0.001	10ms	50	500	Waveguide horn - directional	13k	—	(2.45GHz)	50V/m at 15m	2k	Yes 5 minutes
Low Tech portable UWB [c]	20	300ps	1.5k	10	TEM horn - directional	25M	90	300MHz – 4GHz instantaneous	12kV/m at 2m	85k	Yes 20 minutes
Low tech mobile HPM (radar)	2	1us	400	800	Offset fed parabolic reflector – directional	70M	—	(1.2 to 1.35GHz)	450V/m at 100m	140k	—
Low tech mobile UWB (TED)	90	*500ps**	1k	45	TEM horn - directional	110M	100	500MHz to 4GHz instantaneous	20kV/m at 10m	156k	*Yes 5 minutes*

Table 5: Summary of 'Low tech' disruptor systems

(a) Since the gain or directivity factor of some antennas is complex (i.e. IRA) this quality factor has been derived by Baum [Baum, 1992], See Appendix A
(b) Portability and mobility implies battery or portable prime power operation which is naturally burst limited
(c) Refers to a simulator developed using Low Tech means [Hoad, 1998]

*Values in italics are assumed values using best available knowledge

Source type	Peak power at antenna (MW)	Maximum Pulse width	Maximum p.r.f (Hz)	Average power at antenna (W)	Antenna type	EIRP peak (W)	Rise time (ps)	Frequency spectrum (operating frequency)	Measured or (Calculated) E-field	$r\,E_{far}$ [a] (V)	Burst limited? [b]
State of the art portable UWB (HRR)	0.007	3ns	600k	12.5	Monopole – omnidirectional	11k	—	15MHz – 400MHz instantaneous	*600V/m at 1m*	1.8k	Yes 20 minutes
State of the art portable DS (DS110)	250	4ns	5	5	Multi turn coil – omni directional	500M	—	(375MHz ± 20%)	125kV/m at 1m	380k	Yes 20 minutes
State of the art mobile HPM 1 (Orion)	350	500ns	100	17.5	reflector – directional	9G	—	(1 to 3GHz) with separate tubes	30kV/m at 75m	1.6M	10s
State of the art mobile HPM 2 (MTF S-band)	140	400ns	300	17	Cassegrain - directional	5G	—	(2.86GHz)	80kV/m at 15m	1.2M	10s
State of the art mobile HPM 3 (MTF L-band)	25	5us	1k	125	reflector – directional	500M	—	(1.3 to 9GHz) with separate tubes	30kV/m at 15m	385k	10s
State of the art mobile DS 1 (DS350)		*10ns*	5		Multi rod dipole omnidirectional			(50 MHz 60MHz and 100MHz) tuneable	300kV/m at 1m	300k	—
State of the art mobile DS 2 (Kekez)	100	70ns	50	350	—	160M	—	(31MHz, 86MHz, 146MHz and 249MHz)	145kV/m at 1.7m	217k	—
State of the art mobile UWB (JOLT))	11	400ps	600	3k	HIRA – directional	14G	150	500 MHz – 2GHz instantaneous	80kV/m at 85m	2M	1s at max p.r.f
HEMP (E1) [c]	50,000	20ns	1	1M	Nuclear detonation	5T	1000	0 to 200MHz	50kV/m	1.5G[d]	One shot

Table 6: Summary of State of the art disruptor systems

(a) Since the gain or directivity factor of some antennas is complex (i.e. IRA) this quality factor has been derived, See Appendix A
(b) Portability and mobility implies battery or portable prime power operation which is naturally burst limited
(c) From reference by Ianoz [Ianoz, 2000]
(d) Assuming 30km Height of burst

*Values in italics are assumed values using best available knowledge

2.3.4.4 Conducted Disruptor Systems

As stated previously EM conducted disruptors exploit the conductive paths to the victim. Simplistically any high voltage generator or pulsed power system can be used to drive high voltages or high current into conductors such as cables attached to or adjacent to the victim system.

For Low Tech conducted disruptors no complete systems could be found in the open literature. However, Tesla coils have been manufactured with outputs up to 14 Million Volts at 85 kHz. Other Low Tech examples could include Tazers or car ignition systems.

For the state of the art many systems such as damped oscillatory wave, surge, and even lightning impulse generators exist for EMC, lightning and HEMP testing. An example of one type is the Electrical Fast Transient (EFT) generator test set. This generator is capable of producing a 4kV impulse with a rise time of 0.5 ns and a pulse width of 50 ns. Another example is the Repetitive Random Square wave Pulse Generator (R2SPG), developed for military conducted immunity tests in the United States [Hoeft, 1994]. The generator parameters are not provided. More powerful mobile conducted HEMP generators have been developed in the FSU [Golikov, 2002]. These mobile simulators are known as 'Zenit-A', and 'Zenit-K'. Table 7 shows the specifications for the two sources.

Output Parameters	**Zenit-A**	**Zenit-K**
Voltage pulse amplitude	100 to 800 kV	10 to 35 kV
Voltage pulse rise time	10 to 80 ns	3 to 10 μs
Voltage pulse width	0.5 to 5 μs	Up to 100 ms
Current pulse amplitude (short circuit)	20 kA	Up to 80 kA
Current pulse width (short circuit)	Up to 1 μs	Up to 70 μs

Table 7: Very powerful mobile conducted simulators

There appears to be less discussion in the literature concerning EM disruptors which exploit the conductive channel to the victim. This seems counter-intuitive since it has been shown (Appendix A, Section 6.2.3) that the conducting channel may offer lower path loss (less attenuation) than the radiating channel.

2.3.5 Summary of EM Disruptor Sources

From the discussion above the following summary has been drawn:

- The main design goal for the disruptor designer is to optimise the energy delivered to the victim system
- A secondary goal is to optimise and faithfully radiate or inject the modulated pulse characteristics
- The type of components and primarily the modulator type used define the disruptor type
- The disruptor can produce a single pulse or repetitive pulse trains although the latter is likely to be limited to a burst of a few seconds duration
- The capability of the disruptor manufacturer can vary from Low Tech through to state of the art
- Four classes of deployment scenario for EM disruptors have been considered, although the man portable and mobile scenarios are more likely for the lower capability groups
- There is sufficient 'open source' discussion to derive parameters for Low Tech and state of the art EM disruptor systems
- Low Tech disruptor designs are available on the Internet, however, a review of the designs shows that they are unsophisticated and rudimentary and even dangerous for an amateur to attempt to manufacture
- High voltage or high current pulse generators capable of exploiting the conductive channel have been summarised but fewer examples have been found in the literature

Some of the quoted unique features of EM disruptor weapons over conventional weapons are:

- Deep magazine – a military term referring to the fact that the ammunition (effectively electrical energy) is available as long as the prime power is available
- Speed of light attack – the disruptor wave front will propagate through air or along cables at the speed of light compared with conventional ballistic ammunition

- Rapid re-targeting – It is possible to engage several targets in quick succession by moving the antenna
- Non Lethal – Does not kill people[7]

Direct inter-comparison of sources from different classes of EM disruptor is difficult because of:

- The different characteristics of the waveform types produced
- The effect these characteristics may have on the victim system
- The deployment scenario of the disruptor

This section has highlighted the complexity and in some cases the operational constraints of complete Low Tech and state of the art EM disruptor systems and simulators.

2.4 EM Disruptor Effects/Susceptibility Open Source Data

2.4.1 Radiated Disruptor Effects

Sub system level susceptibility i.e. the susceptibility of discrete components and circuits is widely discussed in the open literature [Sonnemann, 2003], [Demoulin, 1995]. However, a component or circuit response to EM disruption is difficult to interpret from a system level effects study because the circuit coupling will be severely modified by the system enclosure. Indeed EMC design allows for the incorporation of containment or shielding at the enclosure or system level. The shielding provided by the enclosure is likely to have a large bearing on the overall system susceptibility threshold. Susceptibility evaluation at the sub system level therefore invalidates or at least does not account for some of the protection measures built in to the design of the overall system. Also, information *systems* are the focus of this study therefore system level effects will form the majority of this discussion.

There are very few openly published papers which discuss in sufficient details system susceptibility to high power EM simulators. The few published accounts appear to be military led research programmes aiming to understand electronic system susceptibility to High power EM for hardening, protection and survivability purposes.

[7] In this context we are comparing EM disruptors with conventional munitions. Certainly high power RF exposure can harm humans and potentially lead to long term health effects.

The earliest accounts in the open literature discussing susceptibility and effects of systems are, unsurprisingly centred on HEMP interaction [Lee, 1986]. However, this data largely pre-dates the use of complex digital systems and microelectronics used for information systems. This and other discussion [Middlestead, 1987] does allude to the fact that HEMP can induce susceptibilities in satellite systems although no absolute values of satellite system effects are provided.

Aircraft electronic (avionics) systems have also been the subject of extensive susceptibility studies [Larsen, 1998], [Fuller, 1990]. The reasons for this appear to be due to several factors.

- Avionics generally employ 'high end' electronics
- Electronic flight control systems perform safety critical functions and must therefore have a high degree of immunity from interference
- The EM environment in which the aircraft is required to operate is severe, due to airport radar, high power RF broadcast transmitters etc.

Military and civil aircraft are evaluated for EM immunity at extremely high levels up to several kV/m in the microwave band. This is interesting since it highlights the fact that safety critical systems can be protected from high power EM environments. However, the relevance of avionics susceptibility to information systems susceptibility is difficult to interpret.

The first highly relevant article containing upset thresholds of computer systems was published in 1999 [LoVetri, 1999]. In this paper standard EMC type TWT amplifiers were used to illuminate three separate tower computer systems via a standard double ridge waveguide horn antenna. This test configuration broadly simulates microwave Hypoband type waveforms.

The distance between the antenna and the System Under Test (SUT) was 1 m, the maximum achievable peak field level was quoted as 100 V/m. A variety of modulation types and antenna polarisations were used. The SUT was exercised, processing data and video images and reading/writing to the hard disk. A variety of upset types or effects were observed including.

- Loss of data
- Reset (where the computer re-started automatically)
- Disk Write error (reported by the operating system)
- Loss of hard disk access (reported by the operating system, power down required)
- Power down (computer shuts down)

The upset thresholds for various SUT types are reproduced in Table 8:

SUT Type	Carrier Frequency (GHz)	Upset threshold (V/m)	Modulation used	Effect
133 MHz Pentium	1.133	50	AM*	Reset
	1.133	50	Pulse**	Reset
	2.675	50	AM	Loss of Access
	2.675	75	Pulse	Loss of Access
	2.713	30	CW***	Loss of data
	2.770	50	AM	Loss of data
	2.887	75	AM	Loss of Access
233 MHz Pentium II	1.070	100	Pulse	Disk Write error
	1.460	100	CW	Power down
	1.460	100	AM	Power down
	1.460	100	Pulse	Power down
	1.480	100	CW	Power down
300 MHz Pentium II	1.040	45	Pulse	Power down
	1.400	100	CW	Power down
	1.43 to 1.55	50	Pulse	Power down
	1.510	100	AM	Power down
	1.510	75	Pulse	Power down
	1.515	100	AM	Reset
	1.690	85	Pulse	Power down
	1.750	75	Pulse	Power down

Table 8: Minimum radiated susceptibility threshold of computers, after LoVetri et al
*AM – Amplitude modulation with 80% modulation depth
**Pulse – 217Hz, 50% duty cycle (2.3ms Pulse width)
***CW - Continuous wave i.e. no modulation applied

This table is therefore indicative of upset thresholds for computer systems from a microwave Hypoband type disruptor.

Other important sources of susceptibility data are provided by Backstrom [Backstrom, 2004] of the Swedish Defence Research Organisation, Camp [Camp, 2004], of the

University of Hanover, Germany and Nitsch [Nitsch, 2004] of the German Ministry of Defence (MoD).

Backstrom has evaluated a variety of systems for susceptibility against Hypoband (HPM) using the MTF facility described earlier and other conventional techniques. Systems tested appear to include, motor vehicles, computers, monitors, card readers, missiles, radios and telecommunications systems. Of these it is remarked that flat screen monitors were damaged at 100V/m at a pulse repetition frequency of 1 kHz and a pulse width of 0.5 ms (50%) duty cycle, the centre frequency appears to be 140 MHz. The card reader was disturbed at 80V/m using the 1.3 GHz MTF, the upset type was to 'lock out' users [Backstrom, 2002].

For the motor vehicle (a 1993 model) it was observed that engine stopping occurred at 500 V/m at 1.3 GHz to 3 GHz with a 5 μs pulse width and 200 Hz pulse repetition frequency. Damage occurred at 15 kV/m (1.3 GHz) and 25 kV/m (2.86 GHz). Damaged components included engine control units and relays [Backstrom, 1999]. General observations by Backstrom include:

- System susceptibility effects are more prominent for HPM in the 1 to 3 GHz region than the 5 to 15 GHz region
- Upset in the 1 to 3 GHz region starts to occur around a few hundred V/m (theoretically evaluated at 300 V/m)
- Permanent damage in the 1 to 3 GHz region starts to occur at 15 to 25 kV/m
- Permanent damage can occur with the system turned off (un-powered)
- Damage to Telecommunications receiver components (Front door coupling) at field strength of 2kV/m

Backstrom uses the 300 V/m (upset) and 15 kV/m (damage) values as a benchmark for system susceptibility to microwave Hypoband type waveforms. However, it must be assumed that these magnitudes are only valid for the modulation scheme and the particular test configuration used.

Nitsch, has evaluated the susceptibility of Logic devices, Micro-controllers, computer Motherboards, computer systems and networks. Hyperband (UWB), EMP, and Hypoband waveforms have been generated although specific details of the generator

system are not provided. The Hyperband and EMP tests have taken place in a TEM waveguide, E-Field strengths of 50 kV/m for EMP and 100 kV/m for the Hyperband waveform were achieved. The Hypoband tests appear to have taken place in a reverberation chamber where the maximum field achievable is 4 kV/m. As stated previously the most interesting data for this study is that for computer systems and networks. The computer systems appear to have been tested to Hyperband waveforms only. Three different specifications of computer system (386 25 MHz, 485 33 MHz, and 486 66 MHz) were tested. However, the hard disk for these systems was removed for the test and an external cable was attached to monitor the Direct Memory Access (DMA) controller and Programmable Interval Timer (PIT) module. This cable is likely to have violated any EM shielding provided by the system enclosure.

The upset criteria are not precisely defined but appear to relate to incorrect program function after interrogation. The upset threshold (Nitsch uses the term breakdown threshold (BT)) for the three systems is given in Table 9.

SUT Type	**Modulation**	**Average Upset threshold**
386 25 MHz	Hyperband (t_r = 100ps, t_{fwhm} = 2.5ns, repetition rate unknown)	17 kV/m
486 33 MHz		13.5 kV/m
486 66 MHz		12 kV/m

Table 9: Minimum radiated susceptibility threshold of computers after Nitsch et al

This data appears to indicate that the more modern systems are more susceptible to the Hyperband threat. However, it is very unclear whether the computers evaluated for this study were complete systems (i.e. whether the computer motherboard was within an enclosure).

For the computer networks study only the cable was illuminated with the EM stress with the computer terminal systems effectively screened using absorber walls. This situation is very unlikely to occur in a realistic scenario since the systems connected to the network will be at least partially illuminated. The results of the minimum upset thresholds for various conditions are as shown in Table 10.

Upset Type	Modulation	Minimum Upset threshold
Bit errors	Hyperband (t_r = 100ps, t_{fwhm} = 2.5ns, repetition rate unknown)	200 V/m (10 Base 2)
Lost frames		4 kV/m (10 Base T)
Network Upset (Denial of Service)		6 kV/m (10 Base T)

Table 10: Minimum radiated susceptibility threshold of networks after Nitsch et al

Again the actual repetition rate at upset is not given. However, it is stated that the number of lost frames increases linearly with increasing repetition frequency. The range of repetition frequencies available is 1 Hz to 200 Hz [Mojert, 2001]. It was also observed that shielded network cable types, Shielded Twisted Pairs (STP) offer more protection than unshielded types.

In another study [Nitsch, 2005] Nitsch evaluated the susceptibility of complete computer systems to EMP and Hyperband, again with the TEM simulator. Table 11 provides a summary of this work.

SUT Type	Modulation	Average Upset threshold
AMD K6 300MHz	EMP1 (t_r = 10ns, t_{fwhm} = 400ns	16 kV/m
	EMP2 (t_r = 1ns, t_{fwhm} = 25ns	7 kV/m
	Hyperband1 (t_r = 100ps, t_{fwhm} = 2.5ns	3 kV/m
Pentium II MMX 350MHz	EMP1 (t_r = 10ns, t_{fwhm} = 400ns	40 kV/m
	EMP2 (t_r = 1ns, t_{fwhm} = 25ns	12 kV/m
	Hyperband1 (t_r = 100ps, t_{fwhm} = 2.5ns	7.5 kV/m
Pentium II 400MHz	EMP1 (t_r = 10ns, t_{fwhm} = 400ns	9 kV/m
	EMP2 (t_r = 1ns, t_{fwhm} = 25ns	6 kV/m
	Hyperband1 (t_r = 100ps, t_{fwhm} = 2.5ns	4 kV/m

Table 11: Minimum radiated susceptibility threshold of computers to HEMP and UWB after Nitsch et al

Nitsch points out that the effective susceptibility threshold of the SUT's is affected by the pulse characteristics of the waveform. Indeed the susceptibility threshold for the fast risetime, narrow pulse width Hyperband pulse is lower in all cases than the susceptibility threshold for the slower rise time longer duration EMP pulses. This is perhaps counter intuitive since the effective energy in the Hyperband pulse is much less than that of the EMP pulse. However, it is shown that due to the higher frequency content of the Hyperband pulse the waveform couples more energy into the SUT geometry i.e. the Hyperband waveform has a higher coupling efficiency for the specific SUT geometry.

Camp, has evaluated the Hyperband waveform susceptibility of micro-controllers and different generations of computer motherboards from 8088, 5 MHz technology through to Pentium III, 500 MHz technology. The same TEM simulator used by Nitsch was used for this research. The general trend observed by Camp is a reduction in the susceptibility threshold for the newer technologies, from 21.6 kV/m for the 8085 to 3.2 kV/m for the Pentium III. This trend appears to concur with the prediction that as technology moves forward devices become more susceptible. However, it should be noted that these tests were carried out on exposed motherboards which were not integrated within an enclosure. It is well known that containment or shielding is an effective EMC design technique which could perhaps mitigate this fact.

Liu Di-Chen et al [Liu Di-Chen, 2003] from Wuhan University in China have conducted a radiated susceptibility study of computer systems. The EM disruptor simulator used for this study appears to be a lightning impulse generator with the parameters (t_r = 2.6 μs, t_{fwhm} = 50 μs). The radiating structure appears to be a simple sphere-sphere spark gap. The type of computer, age and specification are not provided but the following effects were observed, Table 12.

Upset Type	Modulation	Minimum Upset threshold
Mouse pointer deflection	(t_r = 2.6μs, t_{fwhm} = 50μs, single shot)	800 V/m
Momentary upset		6.4 kV/m
Latch up		12 kV/m
Damage		14.2 kV/m

Table 12: Minimum radiated susceptibility threshold of computers to DS after Liu Di-Chen et al

The principal conclusions of this paper are:

- The computer case or enclosure offers a fair degree of shielding to the system
- The field penetration is primarily through the mains cable or through apertures
- Upset is much more likely to occur than damage

Hagbae Kim et al [Hagbae Kim, 2000] have studied the effects on computer systems which are part of an unspecified real time industrial control process. In this instance the computer is used to receive and process sensor inputs and thereby modify the operation of the control process. It is well known that standard off the shelf computer systems are now widely used for a variety of control functions from Nuclear reactors to sewage processing plants. The experimental investigation took place in a reverberation chamber, where the entire control system was illuminated. It was observed that upsets occurred at low levels at 525 MHz and 550 MHz, frequencies corresponding with the harmonic length of the control cable. The susceptibility levels are difficult to interpret since they are in terms of the power used to drive the chamber and the probability of upset. However, the principal effects observed by Kim are temporary transient functional upsets leading to closed loop errors.

All of the studies above have attempted to assess the system level susceptibility from available sources and simulators. There appears to have been no effort or at least none revealed in maximising the efficiency of the susceptibility process by developing optimised waveforms. However, one recent study [Jeffrey, 2004] has attempted to optimise disruption to Ethernet network traffic. Jeffrey et al introduces the concept of Hardware Invariant Protocol Disruptive Interference (HIPDI). As the name suggests the aim is to develop an efficient protocol disruptor which is not influenced by the hardware (terminal equipment and cabling). By analysing the fundamental operating frequencies of 100BaseTX Ethernet the authors of the paper identified critical frequencies and modulation schemes which optimise the degradation of the network traffic. This approach has perhaps more similarity with EW jamming techniques. It was found that specifically for Unshielded Twisted Pair (UTP) – Category 5 cable running 100BaseTX Ethernet the frequencies 33, 65, 72 and 86MHz, using 100% 15kHz square wave AM modulation were the most efficient at causing degradation of the network traffic. However, It should be pointed out that the experiment considered differential mode illumination (where the individual wires of the cable were split out) and illuminated in an

optimum configuration. The authors point out that the more realistic scenario is common mode illumination (where the whole cable is illuminated) and where the efficiency will be strongly influenced by the coupling efficiency of the cable and the common mode to differential mode conversion loss. Still, this paper represents a higher level of sophistication above the other susceptibility studies discussed since there has clearly been an attempt to optimise the waveform parameters.

2.4.2 Conducted Disruptor Effects

There is very limited data available on system upset levels from conducted transients. There is some susceptibility data at the sub system level for older systems [Vick, 1997], [Lutz, 1992] However, modern system level susceptibility is of more relevance to this study as discussed earlier. Two separate groups have published limited system level conducted susceptibility data.

Metatech Corp. in the US [Radasky, 2001] used an EFT generator to inject pulses onto the mains cable of a Pentium specification computer. It was found that 2 kV was sufficient to cause disruption (effectively in the form of network denial of service). The source or load impedance is not given but the data quotes an associated current of 11 Amps giving an associated impedance of 180 Ω. The associated peak power for the EFT pulse is 22 kW at the 2 kV susceptibility level assuming a line impedance of 180 Ω.

Another study was conducted by the Naval Surface Warfare Centre, also in the US. The data here is more limited but for this test a Repetitive Random Square wave Pulse Generator (R2SPG) was used to inject on the mains lead of an Advanced Technology (AT) specification computer system. It was found that 13.4 Amps peak to peak was sufficient to cause disruption in the form of 'latch-up' of the computer. The source or load impedance for this experiment is not given. Both of the experiments above were conducted by injecting on the mains lead of the computer in very close proximity (less than 1m) from the SUT. The associated peak power for the R2SPG pulse is 32 kW, assuming a line impedance of 180 Ω, as before, most of the energy is located at 3.5 MHz

There appears to be no open source data providing details of system upset via cable injection or other conducting channels, within realistic scenarios i.e. injection on an actual installation.

2.4.3 Disruptor Effects Summary

From the above discussion and the discussion from Section 2.3.3.1 concerning susceptibility of information type systems it is possible to draw the following conclusions:

- System level effects are complex and manifest in many ways. The information system function (i.e. how it is used and what it is used for) will have a profound effect on the overall impact of the disruptor
- Although the effect varies in severity (temporary upset through to damage) the severity appears to be broadly correlated to the magnitude of the stress
- The magnitude of the electric field is not a metric by itself which can be used to describe the susceptibility threshold of the system since different disruptor waveform parameters (for example Hypoband verses Hyperband) require wildly different E-field magnitudes for upset of similar systems
- There is not a sufficient amount of independently corroborated effects data to make firm conclusions about upset and damage levels

The system level effects discussed above have been evaluated in simulated environments and not related to 'real world' scenarios i.e. the impact of the installation for example has not been considered. However, it is also not practical, possible or even desirable to conduct realistic 'real world' EM susceptibility investigations.

Even though simulated and controlled investigations have been conducted it appears that it was always necessary to modify the system configuration to conduct the investigation. It is well known within the EMC community that the uncertainty or inaccuracy of even a well controlled susceptibility type investigation can be as large as ± 6 dB [Lab34, 2002] (i.e. for a measured susceptibility threshold of 300 V/m the actual susceptibility threshold could lie anywhere between 150 V/m and 600 V/m).

2.5 Open Source Accounts of Disruptor Action

Qualified accounts in the open literature describing the effective use of EM disruptors on electronic systems in realistic scenarios are almost non existent. However, as discussed in the introduction there are many factual accounts of disruption to electronic systems from what could be termed as unintentional disruptors such as the Forestall disaster.

Unintentional disruptors are high power EM systems, such as Radar, RF broadcast transmitters, and natural phenomena such as Lightning.

Schwartau gives a very vivid but undoubtedly fictional account of an EM disruptor scenario in his book 'Information Warfare – Chaos on the electronic superhighway'. In this account a US Navy aircraft fitted with a microwave Hypoband (HPM) disruptor downs another aircraft which refuses to respond to radio communication, in the air. Given the proximities involved the disruptor is much more likely to catastrophically affect the host Navy aircraft (known as fratricide) than any aircraft at range. Schwartau, does however point out a unique feature of the disruptor phenomena, that of 'plausible deniability' of use.

Many accounts highlight the alleged use of an 'HPM Bomb' by the US military, to defeat an Iraqi Radar during operation Desert Storm in January 1991. These accounts are perhaps misinterpreted from reports concerning the widespread use of High speed 'anti radiation' missiles (HARM) such as the AGM-88, which can 'lock on' to radar and other RF emissions [Isby, 1999]. The warhead is a conventional explosive device.

Another account relates to US and NATO use of an EMP or HERF weapon during the Serbian conflict of 1999. This disruptor was allegedly used to disable Serbian communications and create power outages. Again, it is probable that this story is a misinterpretation of reports referring to the first use of special 'soft bombs'. These are based on the BLU-114/B which simply dispensed carbon filaments shorting out overhead power lines [Bender, 1999]. To add to the confusion both of these forms of weapon have been termed by the military as 'electronic attack' where this relates more to the target of the attack rather than the weapon type.

Schriener, a contributor to the US Senate Joint Economic Committee hearings on RFW publicly demonstrated his Low Tech TED disruptor on US National television [Sawyer, 1999], and other demonstrations have also apparently taken place at INFOWARCON '99. During these demonstrations a variety of systems have been targeted. These demonstrations on the whole are fairly unconvincing since they are clearly conducted at short ranges (a few metres), in line of sight of the disruptor and it is possible that some victim pre-selection may have also taken place.

There are several unconfirmed accounts of instances where disruptors have been used against civil systems [The Sunday Times, 1996], [Rosenberg, 1997]. The Times article

indicates that disruptors were used to blackmail a UK financial institution. However, the wording in this article is obscure and could perhaps refer to a more conventional 'cyber' threat.

Another account alludes to the use of an EM disruptor to effect gambling machines (called Pachinko machines) by a Japanese criminal group. Allegedly a suitcase based microwave disruptor was placed next to the pachinko machine, which caused the machine to pay out. Apparently the perpetrator was eventually caught [CSSC, 2004]. Most of the evidence appears to be anecdotal and even if the story is factual the perpetrator was in very close proximity (possibly in contact) with the victim system.

Clear, convincing and documented evidence of disruptor action and effects has not been obtained to date. It is speculated that this is likely to be in part due to a lack of awareness of this form of threat and a lack of deployed detection systems.

2.6 EM Disruption verses Cyber Denial of Service (DoS)

From the above it is perhaps apparent that EM disruption is comparable with cyber type DoS attacks, such as SYN Flood or SYN Ack attacks.

From the cyber DoS attackers' point of view:

- The equipment required to mount a DoS attack is simply the hackers own computer perhaps with some freeware or custom software
- A network can be attacked from a great distance perhaps even from the other side of the world. The attack can be considered to be in band i.e. via internet, wireless, or wired connections
- The victim of the attack will be a corporate network or perhaps a web site
- A good hacker will know if the attack has been successful
- To launch a Distributed DoS (DDoS) attack the lone hacker must cooperate with other hackers or enlist 'zombie' computer slaves
- The effect on the network is non permanent, the network is recoverable once the attack is identified and the channel is closed or filtered

For an EM disruptor:

- The equipment required to mount an EM disruptor DoS attack is fairly sophisticated, requires a level of expertise to build together with facilities for manufacture
- For an effective DoS attack the EM disruptor has to be in proximity (excluding HEMP) to the victim system. The proximity depends on many factors such as the capability of the disruptor source and the level of attenuation offered by the installation (see Appendix A, Section 6.3). The attack is out of band, propagation of the threat to the victim is either through the ether (radiated) or via any conductors
- All types of electronics can be affected by the attack for example electronic access systems, fire alarm systems, and environmental control systems. These could essentially produce a DoS type effect
- The uncertainty in causing the desired DoS effect is high and the perpetrator will likely have no sensation of whether the attack was successful
- The HEMP threat whilst extremely technically sophisticated could produce a very large scale DDoS attack
- The effect can be permanent if damage occurs at least until damaged components are found and replaced

2.7 Features of Disruptor based Threats

Given the above discussions it is clear that electrical and electronic systems could malfunction as a result of applied EM stress from a disruptor. This form of threat is clearly of concern to the availability of information, where information bearing systems or their supporting infrastructure could be upset or damaged.

From the victim information systems perspective, a disruptor system can be:

- Invisible or at least remote
- Insidious
- Indiscriminate

- Non lethal to humans

Crucially, a user of information systems hardware which is subjected to EM disruptor action is unlikely to have any sensation or perception of the EM stress even at magnitudes exceeding RF exposure guidelines for human health [Heynick, 1996]. The user is perhaps more likely to blame faulty hardware, software or manual error, rather than an external EM influence. There is some evidence to suggest that certain individuals can 'hear' modulated microwaves and that others may be 'hyper-sensitive' to EM stress but the exact cause is inconclusive.

The effect of the disruption on the victim information system is:

- Unconventional
- Unpredictable (no effect/temporary effect/permanent effect)
- Indiscriminate
- Un-attributable
- Plausibly deniable

The overall impact of the effect and therefore the risk posed by disruptors depends on the information system function.

It should be noted that from the perpetrators perspective a potential disadvantage in the remote use of an EM disruptor is that there may not be remote indication of whether an attack was successful. Another risk from the perpetrators perspective is that of fratricide, i.e. the use of the disruptor may upset or damage the perpetrators own electrical or electronic equipment. This is particularly relevant to the mobile scenario since the mobile platform could cease functioning unless hardened against the fratricidal effects.

2.8 Mitigation/Countermeasures

Mitigation measures for disruptors can vary from a simple extrapolation from standard EMC techniques such as shielding and filtering to more rigorous and therefore costly approaches [Kopp, 1997]. In principle shielding and filtering can be employed at any level of the system from component through to infrastructure. In the simplest sense this involves controlling points of entry. Other techniques employed can include:

- Zoning of systems
- The use of fibre optics to replace copper cables thus removing potential coupling paths
- Shielding
- Good electrical earth bonding [Rawson, 1997]
- Fitting of Transient Voltage Surge Suppressors (TVSS), Metal Oxide Varistors, or Gas discharge tubes, to suppress high level transients on cables [Lee, 1993]
- Filtering power and communications lines
- Designing in hardening at the system design stage
- Using software techniques such as fault trapping, maskable interrupts, and watchdogs [Coulson, 1998]

Implementation of a physical security barrier or some form of non electronic perimeter control together with appropriate filtering would also be very effective since the magnitude of the disruptor stress waveform diminishes with distance from the source. It should be noted that many of these mitigation measures would provide some protection from the EM interceptor threat discussed in Section 2.2 through reciprocity.

One area of particular concern however, is the protection of electronics from front door coupling and in particular RF receiver electronics. There have been some very recent studies which appear to be starting to address this problem for Hyperband (UWB) disruptors [Krzikalla, 2004], EMP [Kaelin, 2004], and Hypoband (HPM) [Jonsson, 2004]. This is of particular relevance to INFOSEC because of the widespread proliferation of wireless devices.

Methods for the detection and forensic investigation of an EM disruptor based attack do not appear to exist in the open literature.

2.9 EM Disruptor Analysis

The aim of this section is to analyse the threat potential of EM disruptors based on the information gleaned from the open source literature discussed above.

2.9.1 Analysis of Radiated EM Disruptors

RFM sources will not be considered in this analysis because real data do not appear in the open literature. This is possibly because of the technical complexity of effectively radiating the output from RFM systems or because of the constraints on prime power or packaging into a deliverable system. The operational concept or deployment scenario for RFM systems is also difficult to grasp since many of the advantages of EM disruptors (insidiousness, remoteness, plausible deniability, non lethality) would be negated by the use of an explosively driven system.

Another claim for RFM is that shielding is defeated by the explosive action allowing the EM disruption to penetrate EM hardened enclosures. However, since the blast shockwave travels close to the speed of sound and the EM wave front will arrive at the target/victim at close to the speed of light this concept is invalid except perhaps for a multiple RFM strike. These factors probably limit the use of such devices to NSA, but most probably war fighting applications.

This analysis will also not consider data for the HEMP threat. This is primarily because the perpetrator is required to have a very high level of technical expertise and nuclear warhead and ballistic missile technology in order to generate an effective HEMP waveform. HEMP will have a catastrophic effect on infrastructure. HEMP is therefore a very low probability event with infrastructure wide implications which will be excluded from further system level analysis.

It is clear from the discussion concerning published radiated susceptibility testing of computer systems that the actual susceptibility level is much greater than the EMC immunity level for the equipment. This immunity is provided through compliance with the EMC directive (nominally 3V/m for non industrial applications over a limited frequency range). It is also apparent that the modulation and disruptor waveform type have a bearing on the susceptibility level.

From the discussions in earlier sections (and those provided in Appendix A) it is clear that the uncertainties involved in the propagation, coupling, and upset of electronic systems is very large. Still it is useful to have a benchmark which somehow describes the effectiveness of EM disruptors. In order to generate a benchmark the open source data for sources will be compared with the open source data for effects.

Backstrom presents a very succinct set of tables to estimate the 'distance of action' for Hypoband disruptor threats. 'HPM Weapon' is taken to refer to a state of the art Hypoband disruptor and the term 'HPM sabotage' is taken to refer to the use of Low Tech Hypoband disruptor. The tables are based on many Hypoband tests of cars, computers and general 'un-shielded' (i.e. no special protection measures) electronic systems. These tables (Table 13 and Table 14) are reproduced here.

HPM Source	**DISTANCE**			
	A few 10's of metres	500 metres	1.5 km	15 km
Large HPM-Weapon (fixed installation) P = 10GW	*Permanent Physical damage*	*Permanent Physical damage*	*Upset**	*Upset**
Smaller HPM-Weapon (deliverable) P = 100MW	*Permanent Physical damage*	*Upset**	*No effect*	*No effect*

Table 13: Estimated distance of action for State of the art Hypoband disruptors adapted from Backstrom et al

* May cause permanent functional damage

HPM Source	**DISTANCE**			
	In close vicinity	15 metres	50 metres	500 metres
HPM Van (mobile) P = 10MW	*irrelevant*	*Permanent Physical damage*	*Upset**	*Upset**
HPM Suitcase (Man portable) P = 100kW	*Permanent Physical damage*	*Upset**	*Upset**	*No effect*

Table 14: Estimated distance of action for Low Tech Hypoband disruptors adapted from Backstrom et al.

* May cause permanent functional damage

These tables are useful and are based on real effects data. However, the following stated assumptions are used to derive the distances.

- The upset and damage thresholds are based on peak values obtained using the specific modulations of the Swedish MTF sources (300 V/m and 15 kV/m respectively)
- The antenna gain is taken from a reflector antenna with 1 m diameter (gain 25 dB approx.)
- The HPM Van appears to be based on a 10 MW radar transmitter

- The HPM suitcase could actually be a Mesoband source

Clearly given the earlier discussions (Table 5 and Table 6) the source power quoted in Backstrom's tables represents an extrapolation of around an order of magnitude in the present capability of state of the art and Low Tech sources.

In order to evaluate the range effectiveness of the state of the art and Low Tech sources evaluated in this study a similar set of tables will be developed.

The most complete (i.e. where most parameters are known) system susceptibility data from earlier has been used to develop the graph of Figure 20. This graph shows the *minimum* susceptibility threshold for computer systems in terms of peak field strength (V/m).

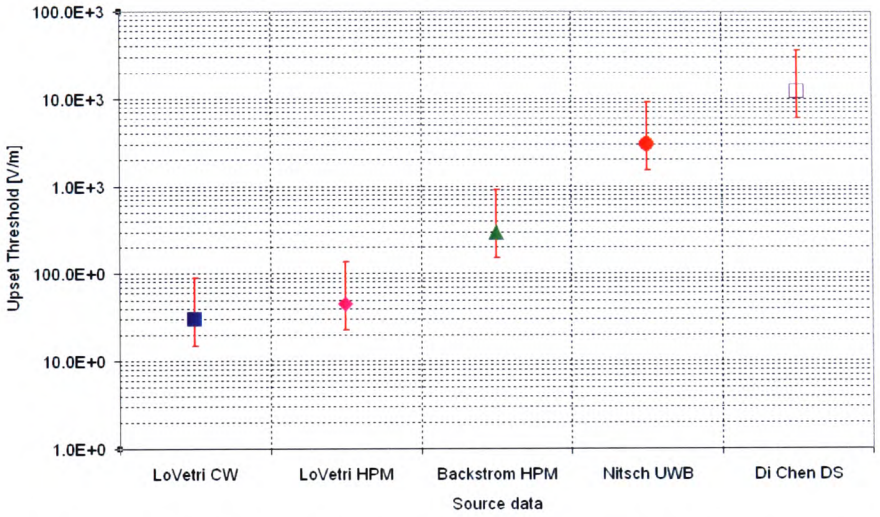


Figure 20: Minimum upset threshold for disruption computer systems as a function of peak field strength

Table 15 shows the minimum upset and damage thresholds for each disruptor class in terms of peak field strength, again derived from the same data set.

Waveform type	**Upset Threshold (V/m)**	**Damage Threshold (V/m)**
Hypoband (HPM)	30	15000
Hyperband (UWB)	3000	No data
Mesoband (DS)	12000	14200

Table 15: Minimum Radiated susceptibility upset threshold for computer systems derived from open source data

There is no data for system damage from Hyperband waveforms this is probably because the damage threshold is either exemplified by very high peak field strengths (100's of kV/m) or because there is insufficient energy within the narrow pulse to cause damage.

It appears from this graph and table that Hyperband (UWB) and Mesoband (DS) are far less effective than Hypoband (HPM) waveforms however, this is an incorrect conclusion since we know that peak E-field strength by itself is not purely deterministic of upset and damage.

It has been shown that perhaps a more effective, but not comprehensive, means of expressing the output of EM Disruptors (RFDEW) is to use the terms peak and average power flux density (expressed in terms of W/m^2) [Nielsen, 1994]. The power density describes the amount of energy per second delivered to the system over an equivalent area (see Appendix A, Section 6.2.1). The average power density is calculated by de-rating the peak power density by a duty cycle factor which accounts for the modulation type, Equation 5.

$$S_{ave} = \left[\left| E^2 / Z_0 \right| \right] * dutycycle \quad \text{.....(Eq. 5)}$$

Where S_{ave} is the average power density in Watts per metre squared

E is the peak electric field required for an effect in Volts per metre

Z_0 is the free space impedance (120π) in Ohms

And *duty cycle* is a dimensionless function of the pulse width (seconds) multiplied by the repetition frequency (Hz)

These equations have been used to derive the upset threshold in terms of the effective average power density (S_{ave}). Figure 21 presents the same data as Figure 20 but this time in terms of effective average power density.

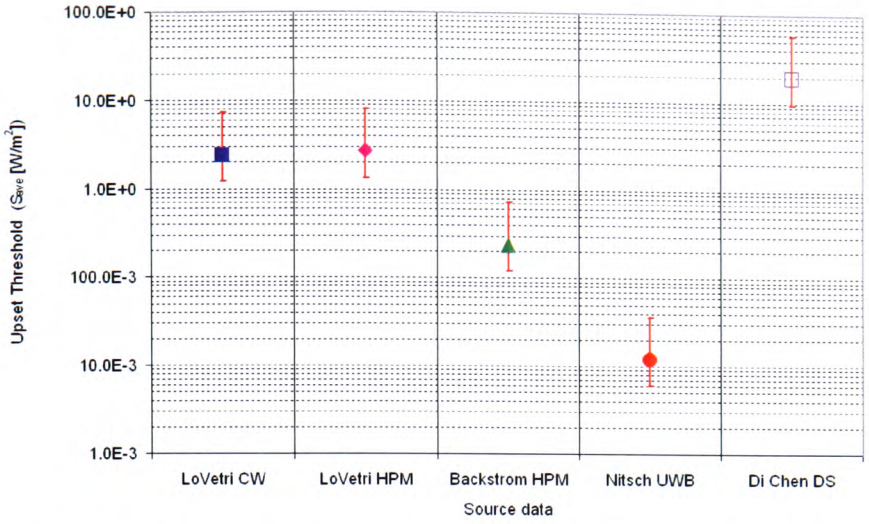


Figure 21: Minimum upset threshold for disruption computer systems as a function of average power density

This figure shows the *minimum* effective average power density required for upset for computer systems using available data. The Hyperband (UWB) waveform now appears to be more efficient than the Hypoband (HPM) disruptor types, a reversal of the earlier peak E-field analysis. This interpretation of effectiveness could be more realistic since it is known that the coupling efficiency for Hyperband waveforms is much greater than Hypoband waveforms because of the very broad instantaneous bandwidth of the Hyperband pulse.

It should be noted that the Mesoband (DS) data has a high uncertainty component since the source drive parameters have been used to derive the upset thresholds rather than the radiated waveform parameters.

Table 16 shows the minimum upset and damage thresholds for each disruptor class in terms of average power density, again derived from the same data set.

Waveform type	**Upset Threshold (W/m^2)**	**Damage Threshold (W/m^2)**
Hypoband (HPM)	0.24	600
Hyperband (UWB)	$12x10^{-3}$	No data
Mesoband (DS)	19	27

Table 16: Minimum Radiated susceptibility upset threshold for computer systems in terms of average power density

The data of Table 16 can be used as benchmarks for upset thresholds for computer systems for each of the different waveform types.

The same average power density equivalence approach as that taken for the effects data can be applied to the disruptor source data presented in Table 5 and Table 6. A reduced set of disruptor sources is given in Table 17.

Source type	Low Tech	State of the art	$r.\ S_{far}$ (i) (W)
Portable Hypoband	☒		5.1×10^3
Mobile Hypoband	☒		21.4×10^3
Mobile Hypoband		☒	2.0×10^6
Portable Hyperband	☒		8.7
Portable Hyperband		☒	15.8
Mobile Hyperband	☒		32.6
Mobile Hyperband		☒	2.7×10^3
Portable Mesoband		☒	7.9
Mobile Mesoband		☒	440

Table 17: Maximum far field equivalent average power density for Low Tech and state of the art sources

(i) For derivation of this term see Appendix A, Section 6.4.4

This table represents the *maximum* average power density produced by each disruptor class. The maximum was found by considering both the peak voltage (r. E_{far}) value and the modulation type. Further, the maximum achievable pulse width and p.r.f, were selected to form the duty cycle factor although it is known that in some cases that this cannot occur due to prime power limitations. Burst length limitations have also been ignored.

Some of the state of the art sources (especially Orion and the MTF) are clearly not feasibly deployable as mobile systems. However, an assumption has been made that these systems could be deployed as mobile systems in the near future. These systems have therefore been classed as mobile systems in the table above. Given these assumptions the data presented in Table 17 represents a realistic prediction of the *maximum* power density which could be produced by disruptor sources.

Based on these assumptions the following estimates of the free space (see Appendix A, Section 6.2.1) effective range, Table 18 through to Table 22 have been calculated.

Low Tech Hypoband Sources	DISTANCE TO VICTIM			
	In close vicinity	15 metres	50 metres	Estimated maximum effective distance
Portable	*upset*	*upset*	*upset*	*140m*
Mobile	*Unpredictable 'Near field'*	*upset*	*upset*	*300m*

Table 18: Predicted free space line of sight effective range of Low Tech Hypoband EM disruptor systems

Low Tech Hyperband Sources	DISTANCE TO VICTIM			
	In close vicinity	15 metres	50 metres	Estimated maximum effective distance
Portable	*upset*	*upset*	*No effect*	*25m*
Mobile	*Unpredictable 'Near field'*	*upset*	*upset*	*52m*

Table 19: Predicted free space line of sight effective range of Low Tech Hyperband EM disruptor systems

State of the art Hypoband Sources	DISTANCE TO VICTIM			
	Less than 20m	50 metres	1km	Estimated maximum effective distance
Mobile	*Unpredictable 'Near field'*	*damage*	*upset*	*3km*

Table 20: Predicted free space line of sight effective range of state of the art Hypoband EM disruptor systems

State of the art Hyperband Sources	DISTANCE TO VICTIM			
	Less than 20m	50 metres	1km	Estimated maximum effective distance
Portable	*upset*	*upset*	*No effect*	*36m*
Mobile	*Unpredictable 'Near field'*	*upset*	*upset*	*500m*

Table 21: Predicted free space line of sight effective range of state of the art Hyperband EM disruptor systems

State of the art Mesoband Sources	DISTANCE TO VICTIM			
	Less than 20m	50 metres	1km	Estimated maximum effective distance
Portable	*No effect*	*No effect*	*No effect*	*No effect*
Mobile	*No effect*	*No effect*	*No effect*	*5m*

Table 22: Predicted free space line of sight effective range of state of the art Mesoband EM disruptor systems

It can be seen from this simplified analysis that mobile Low Tech disruptors are likely to be able to upset computer type systems at free space line of sight ranges up to a few hundred metres whereas mobile state of the art disruptors are likely to upset computer systems at several kilometres.

Clearly and rather obviously Low Tech sources have a lower effective range than state of the art sources. As stated previously it is expected that terrorist or criminal perpetrators will have a capability between the two capability extremes (Low Tech and State of the art). Damage seems to be a very unlikely consequence of disruptor action especially for back door effects discussed here.

These estimated maximum effective distances require strong qualification since many assumptions have used in their development. Some of these assumptions and sources of uncertainty are listed below:

- The magnitude of the coupling efficiency of the victim computer system is not known and it is not possible to quantify the bounds on coupling efficiency from the data given. However it has been shown (see Appendix A, Section 6.5) that the

coupling efficiency for a victim system reduces by 20 dB/decade change in frequency outside of the systems resonance region. This represents a reduction in effective range by a factor of 100 for disruptor sources when the resonant region is not know.

- The inherent uncertainty in measurement of peak E-field and modulation (at least ± 6dB approx. discussed earlier)

- Other contributing uncertainties of the experimental set-up used to derive the susceptibility data, such as test set-up, SUT layout and condition, simulator repeatability and SUT type/specification

- The metric used for these calculations is the average power density only rather than other factors such as the peak field strength. As stated the actual mechanism of disruption is very much more complex, Goransson [Goransson, 1999] has seen variations at device level of up to 16dB

- This analysis has been based on back door coupling to computer systems and not on other electronics systems that form part of information systems infrastructure. It has been shown by Backstrom amongst others that for front door coupling damage is possible to RF receivers at km ranges. It is possible to speculate that sensors which use electronics as the sensing mechanism, such as modern digital imaging devices (e.g. CCTV) and many biometric sensors could also be susceptible to front door coupling.

- The prediction assumes clear line of sight propagation with no influence from the external surroundings. A barrier such as a brick or concrete wall, the interaction of reflections from the ground and other structures, or other mitigation/countermeasures previously discussed could easily provide an attenuation of 10 dB (see Appendix A, Section 6.3). This reduces the predicted maximum effective range for mobile Low Tech sources to just a few metres and to a couple of hundred metres for mobile state of the art sources. Clearly the amount of attenuation offered by installations and indeed the system enclosure is useful for understanding margins and further defining the risk posed by EM disruptors.

- Since the *minimum* susceptibility values and *maximum* source values have been used the maximum effective range is likely to be less than that stated given the coupling efficiency argument amongst others.

These estimates compare fairly favourably with published data including the estimates provided by Backstrom if the source extrapolation is taken into account. Still it is apparent from the analysis that Low Tech and state of the art disruptors have the possibility to be effective either as portable sources at close range to the target/victim i.e. deployed inside an installation probably within line of sight of the victim, or as mobile sources directly adjacent to the installation i.e. within a few metres of the outside of the installation.

2.9.2 Analysis of Conducted Disruptors

The analysis of conducted disruptive threats is more complex than the radiated case [Mansson, 2007]. This is because:

- The attenuation, ambient noise, impedance and propagation characteristics of the propagation channel (cable type etc.) are very complex
- There is very limited susceptibility data available
- There is very limited disruptor source data available

For these reasons a series of experiments are necessary to explore the conducted disruptor propagation path and this is outside of the scope of this thesis.

2.9.3 EM Disruptor Summary

A potted history of the developmental routes of EM disruptor technology has been provided. There has been an attempt to capture all of the various terms related to classes of disruptors and to describe the key parameters of the different classes.

EM disruptor source technologies from components to complete systems have been discussed. It has been shown that the disruptor can be of the radiated type (i.e. uses an antenna) or of the conducted type (i.e. injection onto cables) although the latter case appears to be less mature.

The term Low Tech has been used to describe the typical capability of a well funded amateur, hobbyist or hacker with access to commercially available components and some

workshop space. The term state of the art has been used to describe the capability of National Government research departments with all available resource and state of the art facilities.

Further, it is expected that the technical capability of other adversaries such as criminals, terrorists, and NSA's will lie somewhere between these extremes. It is clear from the discussions that all of the essential components and even complete EM disruptor systems are available for the Low Tech perpetrator.

Four deployment scenarios: Man portable, mobile, fixed and deliverable have been considered. However, portable and mobile systems have been the focus of analysis because most data was available for these types.

There is some limited open source data on the susceptibility and effects of EM disruptors on information systems and this has been summarised. Upset mechanisms and effects are very difficult to quantify and compare leading to a very high degree of uncertainty. The manifestation of the upset is also complex which means an effect is not selectable, and there is a high dependence on the system function. It is suggested that the technical complexity and security implications of gathering and presenting this information probably impede the spread of knowledge.

Qualitative analysis has shown that the maximum effective range is therefore very difficult to quantify and is dependant on many uncertain factors as discussed. However it has been shown that the likely maximum clear line of sight effective range for radiated Low Tech disruptors is less than that for the equivalent state of the art disruptor. It has also been shown that the estimated distances would be severely reduced by surrounding structures amongst other factors.

Still it is apparent from the analysis that Low Tech and state of the art disruptors have the possibility to be effective either as portable sources at close range to the victim, i.e. deployed inside an installation probably within line of sight of the victim or as mobile sources directly adjacent to the installation i.e. within a few metres of the outside of the installation.

System damage seems to be a very unlikely consequence of radiated disruptor action for back door effects but perhaps more likely at short ranges for in band front door effects to RF receivers and electronics sensors. These facts are confirmed in the open literature.

Conventional mitigation/countermeasures are probably effective at reducing the likely effective range of the sources discussed although experimentation and further analysis are necessary. Specific methods for the detection and evidence collection of an EM disruptor based threat do not appear to exist in the public domain. There is clearly insufficient data to develop a specification for an EM disruptor IDS.

Clear, convincing and documented evidence of disruptor action and effects in 'real world' scenarios has not been found to date. This is likely to be in part due to a lack of awareness of this form of threat, and a lack of deployed detection systems. Undoubtedly though, the potential impact to information security could be just as catastrophic as classical 'cyber'/ CNA type threats and other physical threats.

2.10 Stage I - Summary

It has been shown that the Electromagnetic (EM) spectrum can be used to exploit the confidentiality, integrity and availability of information systems. Whilst this is clearly the case EM threats are not explicitly considered in the INFOSEC guidelines.

This study has sought to define EM threat types and the effectiveness of the threats in order to assess the risk to INFOSEC. Accordingly three broad classes of the EM threat have been considered and discussed, these are:

- Electronic Warfare – A threat to the confidentiality, integrity and availability of information systems by exploiting the intentional communications channel
- EM Interceptors – Which potentially pose a threat to the confidentiality of information systems by exploiting intentional and unintentional RF emissions
- EM Disruptors – Which potentially pose a threat to the availability of information systems by exploiting victim electronics susceptibility to high level EM interference via intentional and unintentional RF reception

From reviewing the literature it is clear that the discussion concerning the risks to INFOSEC from EM threats are centred on several factors. These factors were given in the introduction and are reproduced here together with qualifying evidence statements.

1. Our reliance and dependence on information infrastructures

Undoubtedly, we have become reliant on information infrastructures or more precisely the electronic systems containing micro-electronic components which facilitate the

modern information infrastructure. The potential vulnerability that this reliance creates is not exclusive to EM threats.

2. The availability of components and the simplicity of constructing systems capable of launching effective EM attacks at all adversarial levels

For interceptor based threats it has been shown that detection of emissions is relatively simple. However, very sophisticated techniques, relatively sophisticated instrumentation, victim system intelligence, and a great deal of technical skill and patience are required to recover the information. Given these findings it is likely that only the most adept with the best resources could mount a successful interceptor attack. Interceptors have some commonalities with the cyber war driving threat.

For disruptor based threats it is clear that components and even complete systems are readily available. A scale of increasing capability of the perpetrator from Low Tech through to state of the art has been assigned and discussed. All of the essential components and even complete systems are available for the Low Tech perpetrator. The effects of disruptor attacks have some commonalities with 'cyber' DoS attacks.

3. The increased vulnerability of information infrastructures primarily through the use of technology

For EM interceptor based threats it has been shown that at close range (tens of metres) detection and reconstruction of intercepted emissions from both modern (post EMC directive) digital and analogue display systems is possible, even within an office environment where there are a number of systems of similar types polluting the spectrum. It has been shown that modern digital display systems are perhaps more vulnerable than older analogue systems.

For EM disruptor based threats there is limited data on the susceptibility of information systems and a great deal of variability or uncertainty concerning upset mechanisms. This makes susceptibility and effects data very difficult to quantify and compare. The manifestation of the upset has also been shown to be complex with a high dependence on the system function. Depending on the system function, upset of electronics can undoubtedly lead to catastrophic consequences. Many authors assert that as technology advances with higher speed microelectronic devices operating at ever lower voltage levels that systems will become more vulnerable to EM disruptor action. Whilst these technology trends are true, supporting evidence which mirrors this trend in system level

susceptibility is scarce. The increasing susceptibility argument is clouded by the inherent uncertainties in gathering the data as discussed.

4. The inadequacy of existing protection measures and the lack of detection devices

Whilst it is true that INFOSEC practices do not explicitly consider EM threats many of the measures proposed for protection from cyber and physical threats will provide some benefit in protecting systems from EM threats. The introduction of EMC directives provides some basic protection since it mandates minimisation of emissions below a certain threshold and that systems should have some immunity from EM interference.

It has been shown that there are many mitigation or countermeasure types which are routinely available and that these measures are likely to be very effective. However, applying protection for protections sake is not a cost effective option. Understanding and balancing risk is a central theme for INFOSEC management.

The use of EM threat detection systems (in concept similar to Cyber IDS) could be a useful first step in providing awareness and understanding the risk to INFOSEC from EM threats. These detection systems could be used to identify where to apply protection measures in a cost effective manner effectively acting as a de-risking element. The deployment of EM threat detectors could be a useful first step towards a diagnosis/forensic aid for EM attacks. Specific methods for the detection and evidence collection of EM threats do not appear to exist in the public domain. There is clearly insufficient open source data to develop a specification for an EM threat IDS.

5. The insidious remote and covert nature and the effectiveness of EM threats

For an EM interceptor threat a very unique feature is that it will be invisible to the information system which is the victim of the attack. Those in rightful possession of confidential information will have no knowledge or sensation that the confidentiality has been breached perhaps until the information is revealed for surreptitious purposes such as blackmail. However, the predicted practical range for Low Tech interceptor attack is only considered to be a few tens of metres and very dependent on the capability of the perpetrator and the attenuation provided by surrounding structures such as the walls of the installation. There are however, several key areas of potential vulnerability which can be exploited and these have been discussed.

For EM disruptor threats it is clear that any type of electrical and electronic system could potentially malfunction as a result of applied EM stress. Information bearing systems or

their supporting infrastructure could be upset or damaged (although for the majority of systems damage has been shown to be unlikely). The unique features of EM disruptors are; insidiousness, unpredictability, indiscriminate, non perceivable by humans, non lethal to humans, un-attributable and plausibly deniable.

Whilst there is limited, clear, convincing and documented evidence of disruptor action and effects in 'real world' scenarios have not been found to date. It is speculated that this is likely to be in part due to a lack of awareness of this form of threat, and a lack of deployed EM disruption detection systems.

Analysis has shown that the effectiveness of EM disruptor threats is very difficult to quantify and is dependant on many uncertain factors. Still it is apparent from the analysis that Low Tech and state of the art disruptors have the possibility to be effective either as portable sources at close range to the victim system or as mobile sources directly adjacent to the installation.

System damage seems to be a very unlikely consequence of radiated disruptor action for back door coupling but perhaps more probable at short ranges for front door coupling to RF receivers and other electronic sensors such as biometric sensors.

Undoubtedly, the potential impact to INFOSEC from EM interceptor and disruptor threats in general could be just as catastrophic as classical 'cyber'/ CNA type threats.

However, due to the level of complexity it seems clear that only very well resourced individuals or groups could mount a successful EM interceptor attack. For this reason and for others discussed above and in order to make further studies more manageable the bulk of the remaining thesis will concentrate on the radiated disruptor threat only.

The need to further understand the risk to INFOSEC posed by EM disruptor threats is evident and the experiments defined in Stage II are therefore necessary in order to prove or reject the hypothesis of this study.

3 Stage II – The EM Susceptibility of Information Systems

3.1 Aims and Objectives

The aim of the second stage was to conduct experiments in order to further refine an understanding of the threat and to enable the formulation of a specification for EM threat detection measures.

Objectives:

- Conduct experiments to assess the radiated susceptibility of computer systems
- Conduct experiments to assess the radiated susceptibility of computer networks
- Summarise findings so that detection concepts can be developed

3.2 Radiated Susceptibility Test methods

Susceptibility testing is complex and requires suitable equipment such as signal sources, amplifiers, antennas and measuring devices, together with a suitable environment to

produce the radiated stress without affecting the measuring equipment or indeed other electronics in the vicinity. Most of the susceptibility tests discussed in Section 2.4 made use of a disruptor source or simulator to radiate the system. Usually, this is conducted in the open air at facilities which are remote from civilised areas. However, this technique has many disadvantages as discussed the main ones being the limited frequency and modulation coverage of the simulators and the uncertainty in the measured data.

An alternative technique is to produce the required radiated stress in a more controlled environment such as an anechoic chamber or a GTEM cell [IEC 61000-4-3, 2006]. These environments are essentially enclosed room like structures with very good shielding properties in which the radiating antenna and System Under Test (SUT) is housed. Anechoic material known as Radar or Radio Absorbent Material (RAM) is used to reduce reflections from the walls of the chamber so that the field from the transmitting antenna predominates.

This test configuration is most commonly used for EMC immunity and susceptibility testing. However, this technique still has many disadvantages:

- In practice the inaccuracy or more precisely the measurement uncertainty associated with the measurement of the stress level on the SUT is still large ±6 dB
- The SUT must be rotated in order to illuminate each side
- The repeatability is poor
- It is difficult to achieve the high stress levels necessary to induce susceptibility using conventional EMC type amplifiers since the RAM absorbs some of the radiated power

An alternative and fairly new technique is to use a reverberation chamber [IEC 61000-4-21, 2003]. A reverberation chamber is a shielded room or closed cavity similar in construction to an anechoic room but without any RAM. This allows for the E field from a radiating antenna to reflect around the chamber causing constructive and destructive interference. In this way 'hot spots', regions of high peak intensity and 'nulls', regions of field cancellation are formed within the chamber. The chamber is equipped with a mechanical tuning/stirring device whose dimensions are significant fractions of the chamber dimensions. When the chamber is excited with RF energy the resulting multi-mode electromagnetic environment can be 'stirred' by the mechanical tuner/stirrer (i.e.

the hot spots and nulls are circulated around the chamber. A photograph of the QinetiQ Large reverberation chamber is shown in Figure 22.

Figure 22: Large Reverberation chamber QinetiQ Farnborough (room H)

A snap shot of the variation of the spatial field intensity is shown in Figure 23.

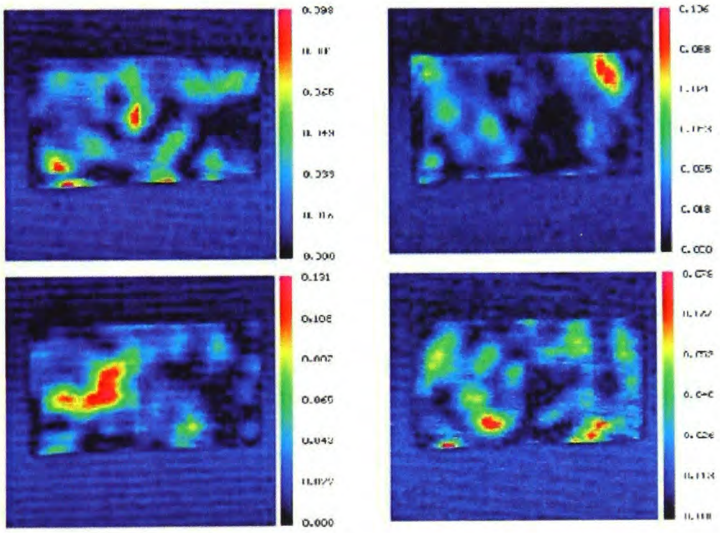


Figure 23: Variation of spatial field intensity inside the QinetiQ Farnborough reverberation chamber (room H)

This 2D image shows regions of varying field intensity with the highest intensity field (hot spots) shown as red. The image was captured by placing a heat sensitive film (coloured region of the image) within the chamber and viewing the heat induced by the RF field via a heat sensitive camera. The images show the effect of four different stirrer on the position of the hot spot within the chamber.

Reverberation chambers have a number of advantages for system testing namely:

i) The field strengths available are much higher per watt of input power than a conventional anechoic room or GTEM cell

ii) The peak field strengths at different locations within the room are more uniform (time averaged over one paddle/tuner rotation) than is possible whilst employing an anechoic chamber/room or GTEM cell

iii) The SUT will be subjected to the peak field levels in a multitude of polarisation's and angles of arrival which is prohibitively time intensive in an anechoic room or open field test site. It has been argued that this is more representative of the true EM environment when the system is within its intended operating environment [Borgstrom, 2004] i.e. the radiated field will be scattered by conductive objects (such as components of desks tables and the building structure including the ground)

iv) All parts or faces of the system will experience the peak field levels over the time for one paddle or tuner rotation. Therefore the particular orientation of the SUT cables has less bearing on the susceptibility threshold

v) The repeatability is better than conventional anechoic techniques due to time averaging which produces a more consistent test method

vi) Most importantly the uncertainty is lower than that of anechoic techniques. Some [Arnaut, 1998], [Musso, 2003] have quoted the expanded uncertainty of the reverberation technique to be of the order of, ± 1.5 to ±1.8 dB at a 95% confidence level

The disadvantages of the reverberation chamber technique are:

i) For mode stirring (i.e. continuous stirrer rotation), the duration that the peak field dwells on the SUT can become an important factor if the cycle time of the SUT is long

ii) Some authors find it conceptually difficult to relate the susceptibility levels recorded using the reverberation method to anechoic, GTEM and open area techniques. This is largely because the technique has only very recently been accepted by the community

iii) The size of the smallest dimension of the chamber dictates the lowest usable frequency at which the chamber can be used

iv) The pulse risetime which can be used is limited by the *Q- factor* of the chamber this restricts the pulse modulations which can be used

v) The directivity characteristics of the SUT are not preserved. This means that the critical illumination angle cannot be revealed and any 'enhancement' in SUT coupling efficiency is cancelled out [Freyer, 2000]

Reverberation chambers have been shown to be a useful environment for achieving a thoroughness of exposure which is difficult to achieve in practice with any other test method.

If further understanding of how a reverberation chamber operates is required then [Hill, 1998] gives a good overview of the subject.

3.3 Reverberation Chamber Susceptibility Test Configuration

The QinetiQ reverberation chambers were the main facilities used to provide a reproducible EM test environment for susceptibility testing. A photograph of a computer under test within the small reverberation chamber is shown in Figure 24.

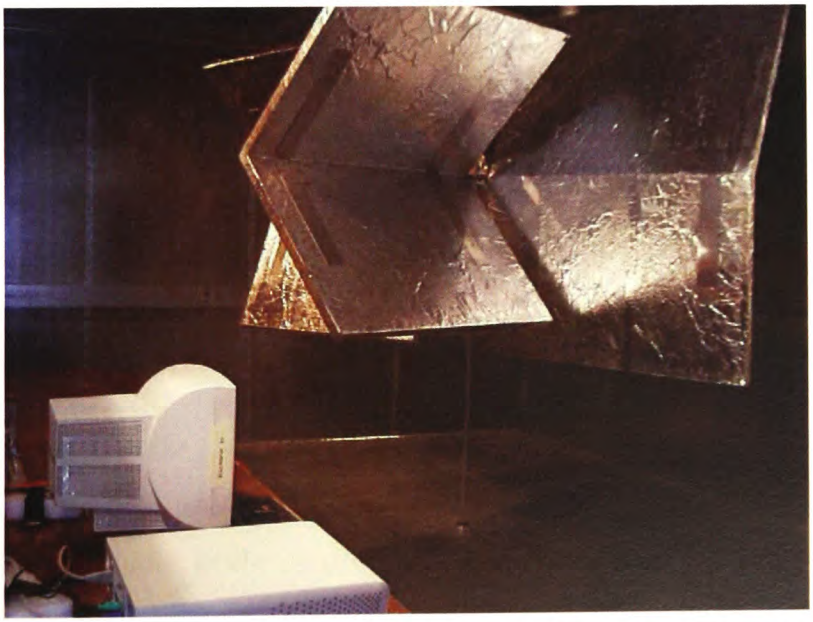


Figure 24: Computer in the QinetiQ small reverberation chamber (room G)

The two chambers used have the following dimensions and minimum frequencies[8] as shown in Table 23.

Room	Width (m)	Length (m)	Height (m)	f_{011} (MHz)	Minimum Frequency ($3 \times f_{011}$) (MHz)
G	5	8	3	35.38	106.14
H	8	10	7	24.01	72.03

Table 23: Chamber dimensions and minimum frequencies

The frequency range selected for the test was 400 MHz to 8 GHz. This was bounded by the dimensions of the chamber and test equipment limitations. The frequencies were stepped through using automatic frequency selection based upon 100 frequency steps per frequency decade, derived by Equation 6.

$$f_{(n+1)} = f_n * 10^{\left(\frac{1}{99}\right)} \quad \text{.....(Eq. 6)}$$

Where f_n is the test frequency and n =1 to 100

f_1 is the start frequency

And f_{100} is the end frequency

From experience gained during previous tests the speed of the mode stirring paddle wheel was set at 3.25 revolutions per minute (rpm). This allows sufficient time for the EM field to dwell and upsets to occur if the field strength is sufficient to do so whilst still enabling all propagation and coupling modes to be assessed during a single test. The cycle time of the computer SUT's is in the order of nanoseconds compared with the millisecond dwell time of the peak field.

At each frequency the EM stress was set to some minimum low level well below the susceptibility threshold of the SUT. The EM stress was effectively allowed to dwell on the SUT for one revolution of the paddle. The magnitude of the electric field was slowly increased until an effect on the SUT is observed. The effect level (susceptibility threshold level) and susceptibility type were recorded via specially designed control software.

The applied stress in terms of E field can be derived from the following Equation 7:

[8] for compliance testing against EMC specification DO160D/ED14D

$$E_c = \frac{8\pi}{\lambda} \cdot \sqrt{\frac{5P_r}{\eta_a}} \quad \text{.....(Eq. 7)}$$

Where P_r is the ensemble average antenna received power

η_a represents the efficiency of the antenna

and λ is the wavelength

For the tests conducted two antenna types were used – a Log Periodic antenna for frequencies between 100 MHz and 1 GHz and a double ridged waveguide horn for frequencies between 1 GHz and 8 GHz. The Log periodic antenna has a quoted nominal efficiency of 0.75 and the horn antenna has a quoted nominal efficiency of 0.9 [DO160D, 2000]. These factors allow for the calculation of the electric field within the chamber via Equation 7.

3.4 Susceptibility Testing of Standalone Computer Systems

3.4.1 Systems Evaluated

The equipment selected for testing comprised of standard commercially available computer systems housed in tower or desktop cases. Several models of computer system were evaluated from different manufacturers. The particular manufacturer of a computer under test has been obscured in order to protect the interests of the manufacturer. These particular systems were selected and tested based primarily on availability. Given the budgetary limitations and the potential for permanent damage to the SUT only older, used equipment was easily obtainable. However the variation of numbers and types enables trends to be developed covering variation in susceptibility with specification/age, technology type, batch and manufacturer.

A brief summary of the computer specifications evaluated is given in Table 24.

Processor Type	Processor clock frequency	Case style	Manufacturer	Number of units
486	66MHz	Desktop	C	1
486	100MHz	Desktop	E	1
Pentium 3	667MHz	Desktop	D	3
Pentium 4	1.4GHz	Mini Tower	C	1
Pentium 4	1.4GHz	Mini Tower	I	1
Celeron	2.6GHz	Mini Tower	D	1

Table 24: Specifications of the computers evaluated

This table comprises eight separate computer systems. An example specification of the manufacturer Brand D computer is: *Desktop Case, 667MHz Intel Pentium 3 Processor, 64MB SDRAM, 10GB HDD, supplied with Windows 98 operating system.*

3.4.2 Test Configuration

To have a reproducible EM test environment the computers were placed one at a time into the QinetiQ reverberation chamber. This allowed for the SUT to be completely, consistently and repeatedly evaluated with every EM illumination angle and polarisation covered equally.

The SUT's were tested in accordance with the QinetiQ reverberation chamber work instruction [P073, 2001]. Thus each of the SUT's were placed on a 4m long conductive test bench installed within the chamber. The 240 V AC mains supply for the computer under test was provided via a Line Impedance Stabilisation Network (LISN). The LISN provides a standard and consistent value for the mains supply impedance aiding test repeatability.

The same monitor, keyboard, mouse and cable layout were used for all computers tested. In this way only the differences in susceptibility of the computer main unit were recorded allowing a fairer inter-comparison. The peripheral wiring (mouse and keyboard cables) for these devices was spaced 50mm above the test bench on Styrofoam blocks so as to further enhance test repeatability.

In order to further improve repeatability the processor and hard disk were set working at maximum capacity. Since it is extremely difficult to predict when this will occur in normal use the computers were exercised using a specialised test program written using Visual Basic. A screen shot of the test programme EMV_101.exe is provided in Figure 25. This figure illustrates that the test program provided consistent 100% CPU usage.

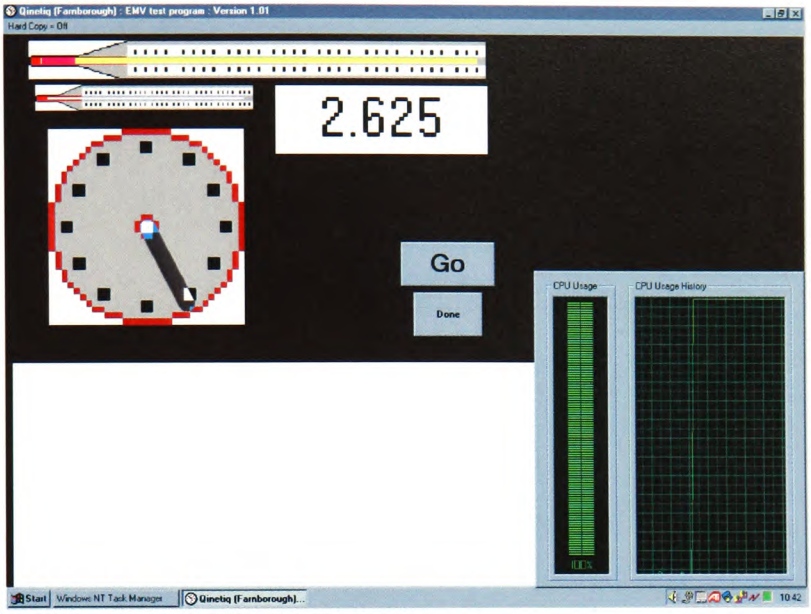


Figure 25: Screen shot of EMV test program Version 1.01

This software continuously carried out a file read/write process on the hard disk. The monitor of the SUT was viewed from the instrumentation/control chamber with a fibre optic linked EM hardened CCTV camera so that the performance of the system could be assessed without compromising the integrity of the test chamber.

The computers were exposed to a simulated Hypoband (HPM) modulation of 30 µs pulse width a 1 kHz p.r.f. This modulation was selected since it was achievable with standard EMC amplifiers. In reality this modulation is representative of a typical Radar pulse but it has been shown that used radar components are available for the Low Tech perpetrator.

The types of effects observed were various and complex but in all cases the magnitude of the stress was increased to a point where manual intervention was required (i.e. where the SUT has to be manually reset). If no effects were observed the EM stress level was taken to the limit of the amplifier in use and recorded as a 'Pass'.

3.4.3 Susceptibility Criteria / Observed Effects

Computer systems are extremely complex and so are the modes of disruption and the types of effects observed. Table 25 is a list of effects observed during evaluation.

Effect	During Exposure to EM Stress	After Exposure to EM Stress
No Effect	No Effect	No Effect
Monitor upset	Blanking or interference	Returns to normal function
Mouse pointer deflection	Influence position	Returns to normal function
Program closure	Pop up menus, program closures, programs moved or deleted	Desktop function may be altered, missing or moved icons
Peripheral crash	Mouse, monitor or keyboard behave erratically	Remove plug to reinitialise or manually reboot
Crash with self restart	The computer stops processing and latches	The computer starts processing again or a soft reset (Ctrl-Alt-Del) is required
Shutdown with self restart	The computer switches off, and attempts to restart without manual intervention	Once EM stress removed the computer restarts normally. During restart operating system detects abnormal shutdown, several files may be affected
'Blue Screen'	An exception error occurs resulting in the customary 'blue screen' error message	The system, generally, can be re-booted without persistent effect
Crash with manual restart	The computer stops processing and latches	During restart the operating system detects abnormal shutdown, several files may be affected
Shutdown with manual restart	The computer shuts down or switches off spontaneously	The computer remains non-functional. During restart operating system detects abnormal shutdown. Several files may be affected
Peripheral Damage	The computer may crash or shutdown	Investigation reveals permanent damage to a peripheral component i.e. monitor, keyboard, mouse etc.
Functional Damage	The computer may crash or shutdown	During restart the computer reports a failure to find the operating system. Re-installation of the operating system cures the fault (expected minimum outage 2 hours)
Physical Damage	The computer may crash or shutdown	During restart the computer either fails to boot or a critical device such as the hard disk malfunctions (expected minimum outage 1 day)

Table 25: Observed effects

It is worth re-stating that the severity of the overall impact of the effect is dependent on the overall function of the system. For example if a process required precise positioning of the mouse pointer e.g. for controlling a crane arm and mouse deflection occurred due to the EM stress then the overall effect to the process could be catastrophic. It should also be noted that the effect observed at any specific frequency is unpredictable. As the stress is increased the effect may change from mouse deflection to shutdown in an approximately linear manner but it was equally observed that the first recorded effect could be any of those listed.

For the data displayed in the graphs below the susceptibility threshold recorded is representative of the cases when manual intervention was required. It was either necessary to manually re-start the test software or to carry out a manual soft / hard reboot of the computer system.

3.4.4 Observations and Test Results

3.4.4.1 The susceptibility of a single computer

The graph of Figure 26 shows the susceptibility threshold recorded for the Brand C 486 66 MHz computer in terms of the total average peak Electric field.

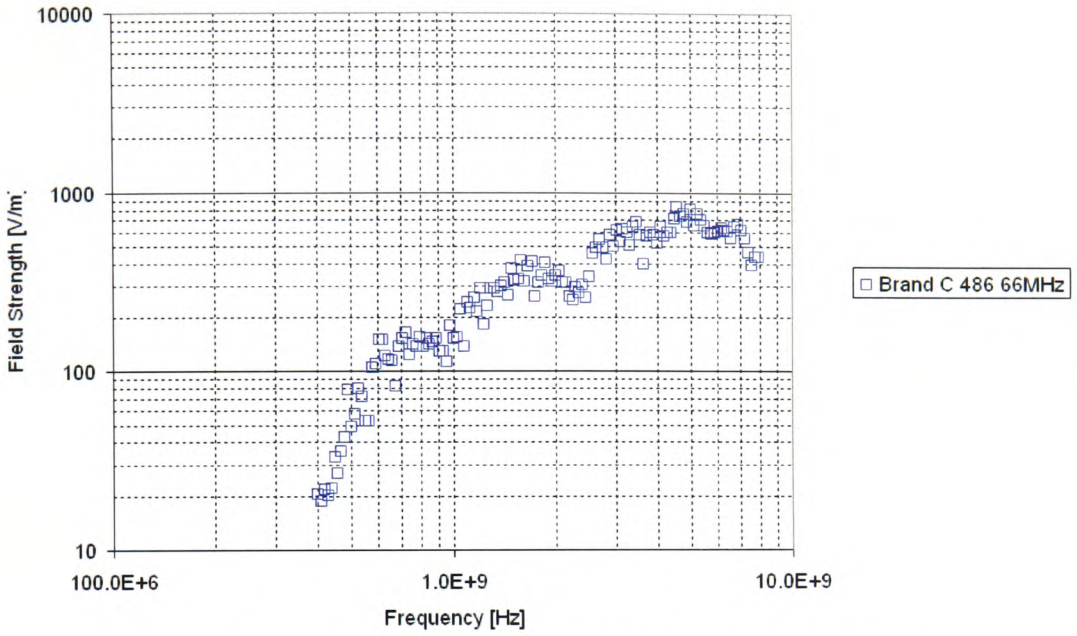


Figure 26: Susceptibility threshold of a Brand C 486 66 MHz computer

Each point on the graph represents a frequency where an effect requiring manual intervention was observed. Frequencies where no effect was observed are not marked. Failure to induce an effect only indicates that no effects were observed at the maximum output of the amplifier in use.

It can be seen from this graph that the susceptibility threshold increases as the frequency increases in the order of approximately 20dB / decade. This indicates that the region of highest coupling efficiency is at the lower end of the frequency range tested. As the frequency increases both the coupling efficiency and rectification efficiency are decreasing leading to an increase in the susceptibility threshold. In practical terms this means that a disruptor source operating at the 400 MHz end of the frequency range would be more effective than one of the same efficiency operating at 8 GHz for this SUT.

Consider the susceptibility threshold graph of the Brand I PIV 1.4GHz computer, Figure 27.

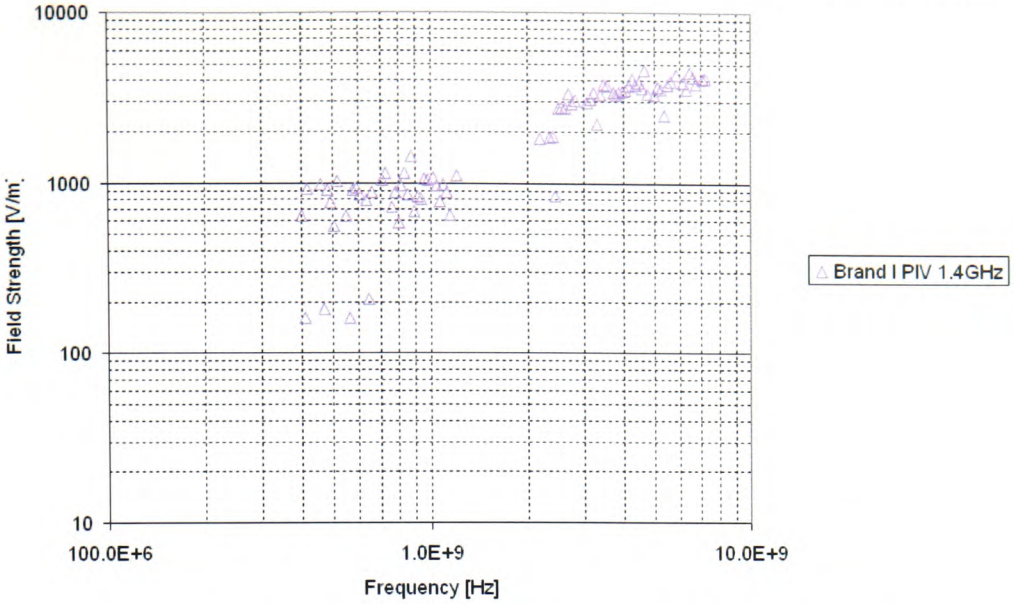


Figure 27: Susceptibility threshold of a Brand I PIV 1.4 GHz computer

It can be seen from this graph that there are greater regions where the effect requiring manual intervention was not achievable with the amplifiers used (no data points) particularly between 1.4 and 2 GHz. In general the susceptibility threshold is also higher than the Brand C 486 66 MHz computer.

3.4.4.2 The impact of batch variation on susceptibility

Three brand D Pentium 3 667MHz computers were procured simultaneously and tested consecutively. These computers appeared to be identical via visual inspection although the serial numbers were non-consecutive. The graph in Figure 28 shows the actual data taken for three nominally identical computers.

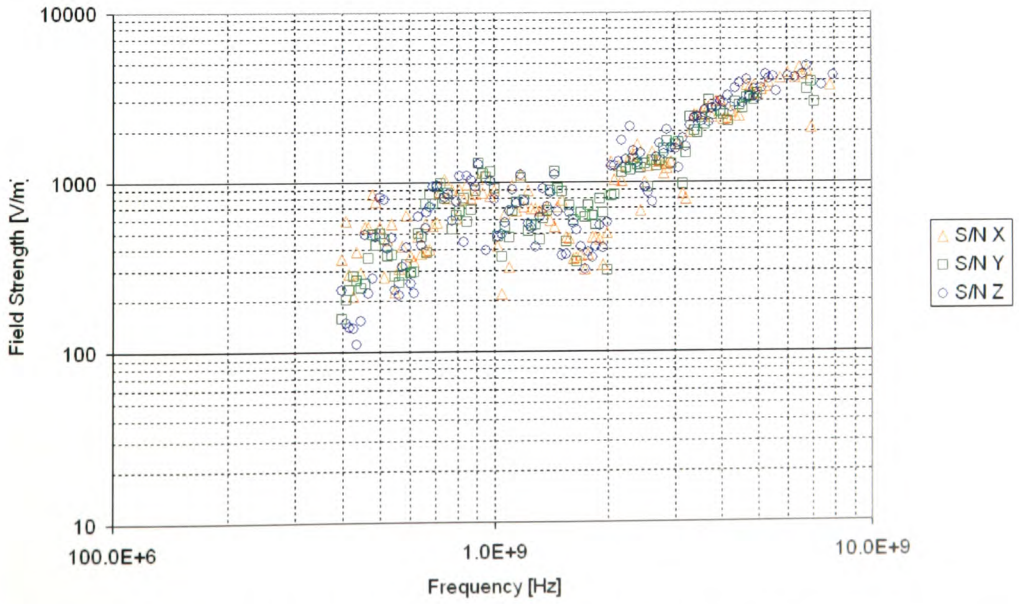


Figure 28: Susceptibility threshold of three same brand and specification computers

Examples of the specific types of effect experienced are listed below:

- At frequencies between 1 and 1.25 GHz the most common failure mode was found to be computer shutdown with self restart/re-boot
- At frequencies above 1.25 GHz the most common failure mode was found to be computer crash with manual restart required
- Mouse deflection was observed intermittently and at lower field strength levels than the other failure modes
- Some minor monitor effects were observed below 1.5 GHz
- A definite increase in susceptibility (i.e. lowering of the susceptibility threshold) were observed around 2 GHz

In order to clarify the trends contained within the graph curve fitting was used to develop simple trend lines. Figure 29 shows different curve fitting options for the data set together with the curve fitting equation and the R^2 correlation value.

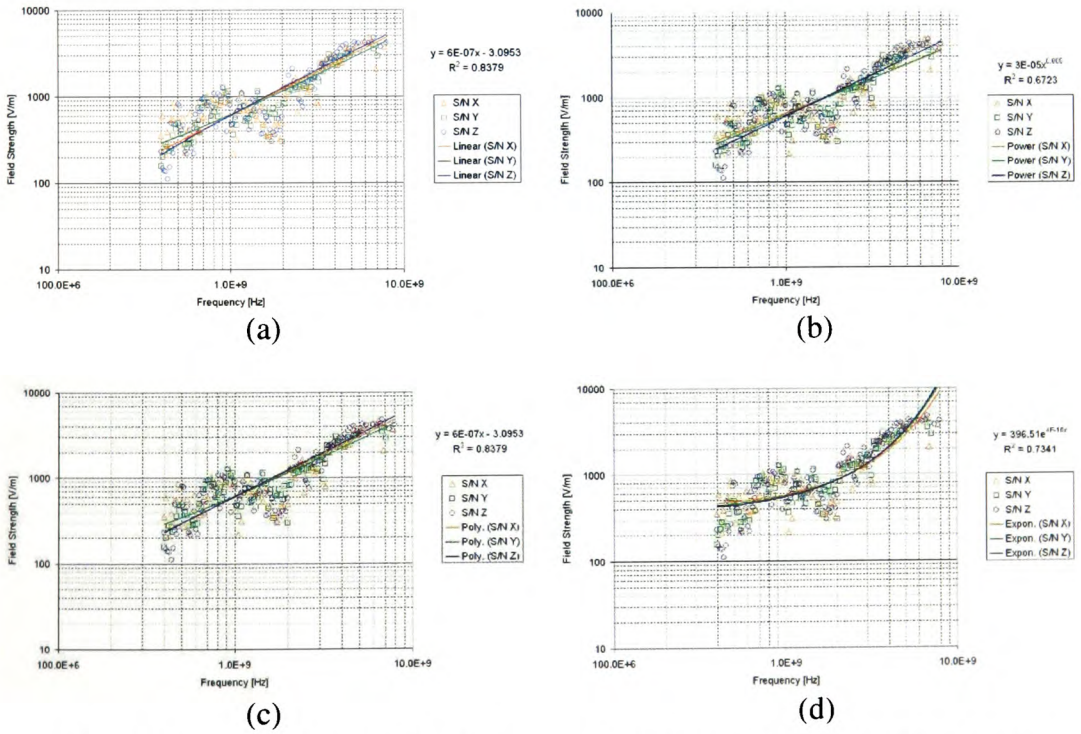


Figure 29: Susceptibility threshold of three same brand and specification computers, raw data with different curve fits trend superimposed

(a) Linear curve fit R2 = 0.8379

(b) Power curve fit R2 = 0.6723

(c) 2nd Order polynomial curve fit R2 = 0.8379

(d) Exponential curve fit R2 = 0.7341

The R^2 value is the Pearson product moment correlation coefficient through the given data points. A value close to 1 represents very good correlation between the fitted curve and the data set and a value of 0 represents very poor correlation.

From this data it can be seen that the linear and 2nd order polynomial curve fits offer the best correlation giving an R^2 value of 0.84. The power curve fit yields a correlation of 0.67 and the exponential curve fit yields a correlation value of 0.7341. The linear curve fitting function in Microsoft Excel was therefore used for further analysis. Figure 30 shows the trend lines in isolation

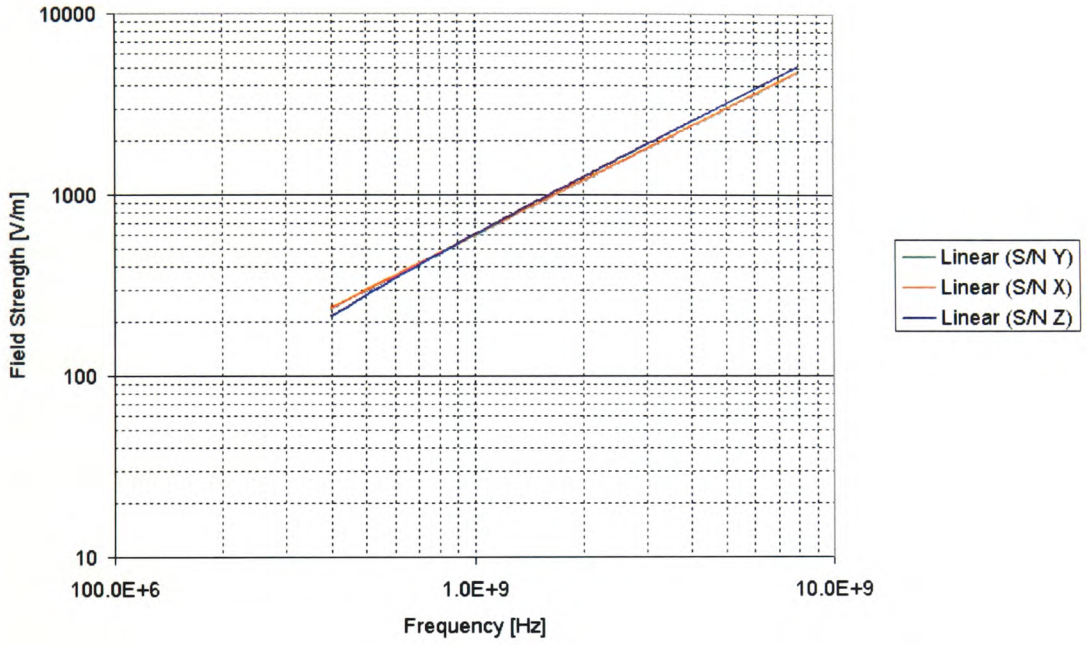


Figure 30: Susceptibility threshold of three same brand and specification computers, trend only

This result is compared with a worst case assumption of the error in the measurement of ±3dB around the mean of the data as shown in Figure 31.

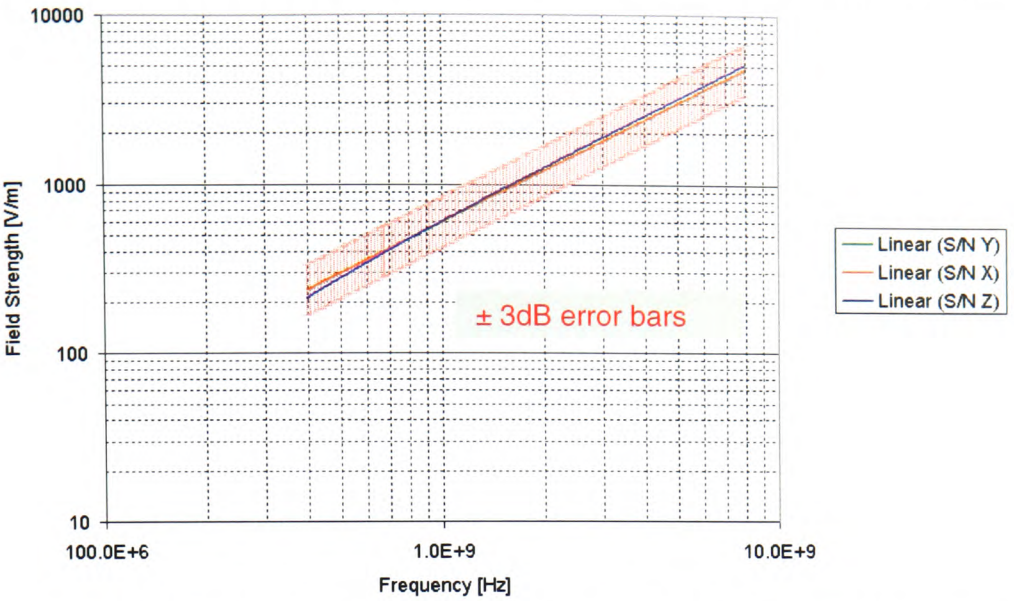


Figure 31: Susceptibility threshold of three same brand and specification computers, trend compared with error bars

The variation of the trend around the mean is well within ±3dB. This not only demonstrates the good repeatability of the measurement method but also shows that the difference in the susceptibility of same brand nominally identical machines is minimal. However, testing of a larger population size would be required to improve the statistical value of this data set.

3.4.4.3 The impact of manufacturer type on susceptibility

Figure 32 shows the susceptibility profiles of two Pentium 4 computers which had identical specifications but were from different manufacturers.

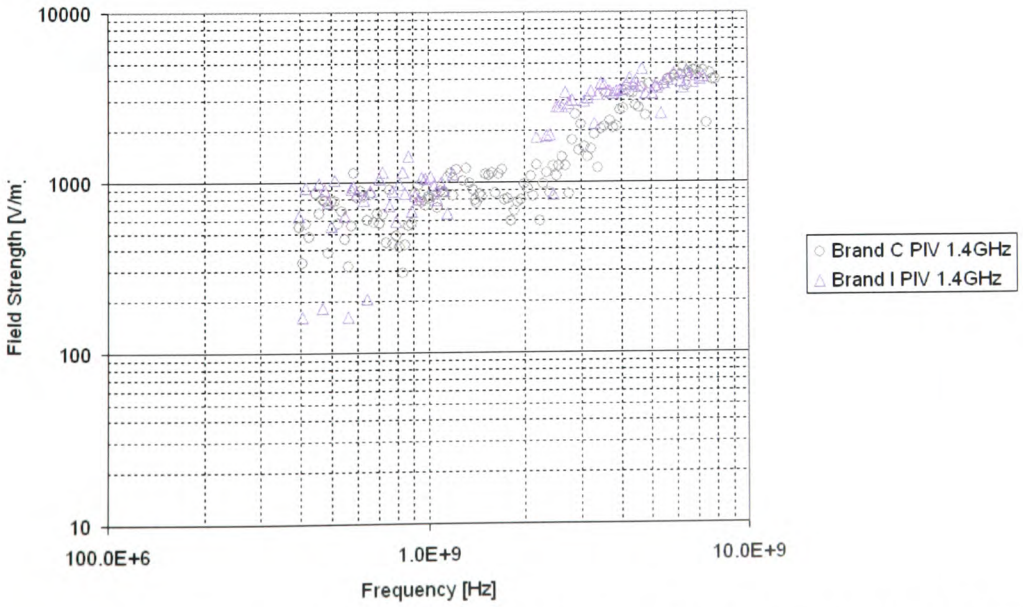


Figure 32: Susceptibility threshold of two same specification computers from different manufacturers

It can be observed that the Brand C computer appears, in general, to be more susceptible than the Brand I computer. Through physical examination of the two computers it was clear that the Brand I computer possessed a slightly better build quality than the Brand C computer. The Brand I computer featured a finger-stock edged case, a metal back-plane and very small apertures around the fan housing. The Brand I computer was also more expensive than the Brand C system. Since the computer case can be used to provide a fair degree of shielding it is apparent that the techniques employed to improve shielding of the brand I system has an impact on the susceptibility threshold.

3.4.4.4 The impact of specification on susceptibility

In order to evaluate the impact of computer specification the remaining computers were evaluated in the same manner. Only the data for one of the Brand D computers and one of the 1.4 GHz specification computers (Brand C) has been included. Figure 33 shows the susceptibility threshold of six computers over the frequency range 400 MHz to 8 GHz.

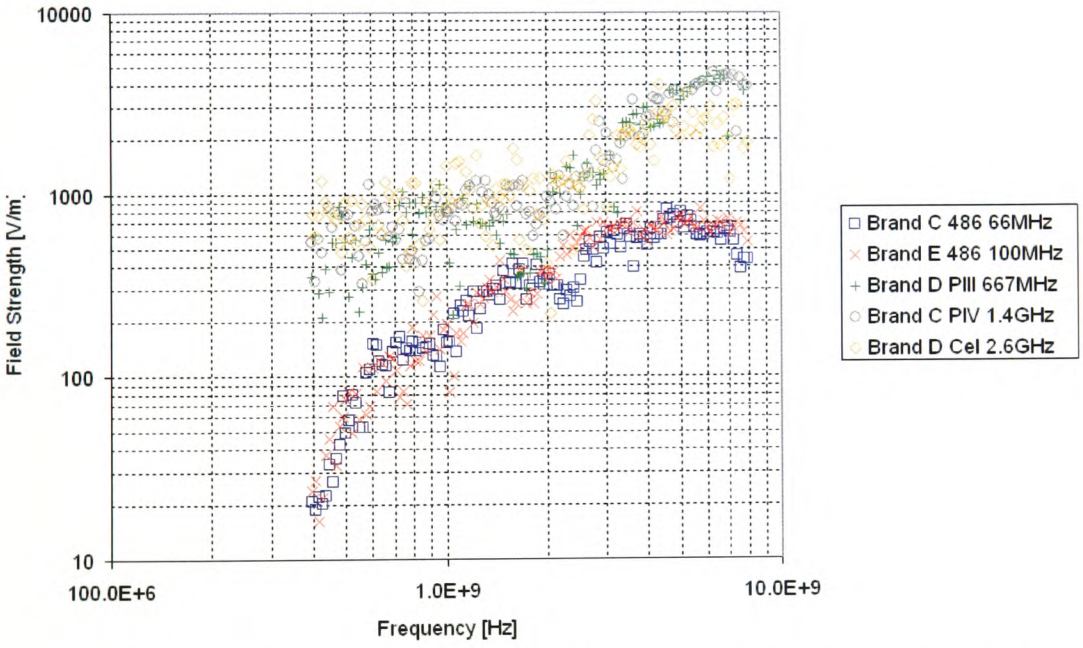


Figure 33: Susceptibility threshold of five different specification computers, raw data

The types of effect experienced and other general observations are listed below:

- The most common susceptibility for the 486 computers was found to be shutdown with manual restart required.
- The most common susceptibility for the Pentium and Celeron computers was found to be computer crash with manual restart required.

- Mouse deflection was observed intermittently and generally at lower field strength levels than the other failure modes.

- Pop up menu activation, program opening and closing and device failure messages also occurred.

- Above 2GHz the CDROM of the Brand C Pentium was found to activate with intermittent opening and closing.

- On several occasions the test program (EMV_101.exe) was closed and moved to a different folder or location on the desktop. Some minor monitor effects were observed below 1.5GHz.

- Compared to the Brand D PIII 667MHz computer definite increases in the susceptibility threshold were observed for the PIV 1.4GHz computers around the clock frequency and the 1st harmonic, 2.8GHz. This probably indicates filtering at the processor clock frequency.

The graph of Figure 34 shows trend lines for the above data set in isolation, using the same curve fitting technique applied to previous graphs.

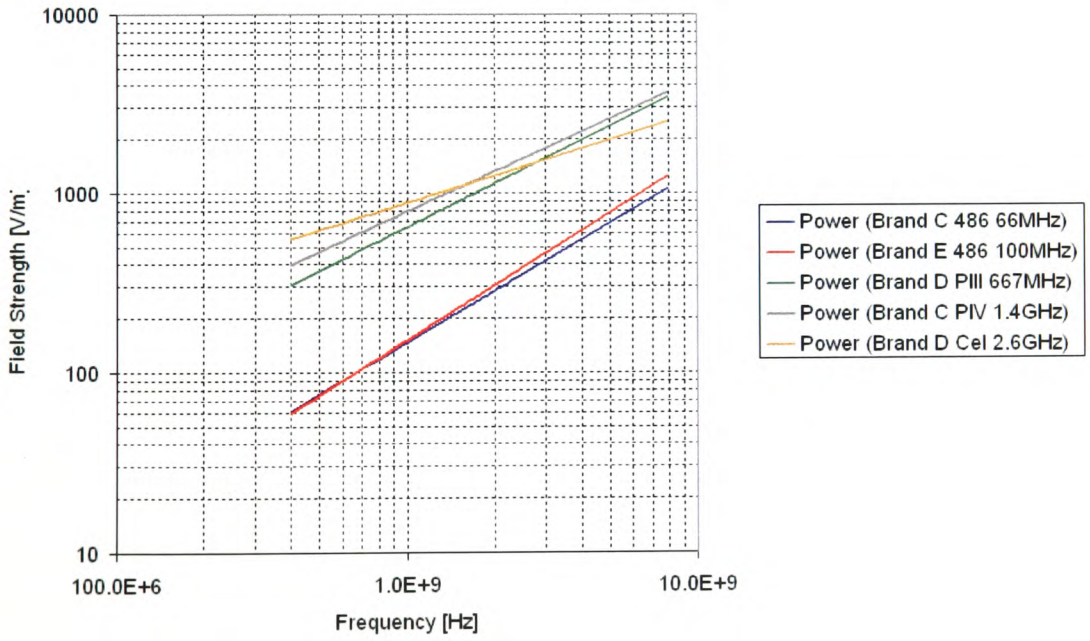


Figure 34: Susceptibility threshold of five different specification computers, trend data

There is clear indication that for any given frequency the susceptibility threshold is much higher for the more modern, higher specification, computer types compared with the older variants. The trend of these graphs shows that modern higher clock speed computers are less susceptible than their older counterparts across the frequencies tested.

There appears to be a minor exception to this trend for the most modern computer tested (Celeron) at frequencies above a few GHz. However, the trend at these frequencies for this computer is skewed by the large variation in the recorded susceptibility threshold data.

This is an important finding and is counter to the belief discussed in Section 2.9.3 that electronic systems will become more susceptible as technology progresses. However, it should be noted that for the Celeron the data spread around the trend line is greater than for the other computers and this has had the effect of skewing the trend line. Still the Celeron computer is still clearly less susceptible than the 486 specification machines. A more detailed discussion of these finding is given in the summary of this sub-section.

There is also indication from the above data however, that build quality has an impact on the susceptibility level. Another observation worthy of note concerns the type of failure modes recorded. In general the faster computers were found to have a more severe reaction to the EM stress. For the Pentium computers 'shutdown' was the most common effect observed. This was usually accompanied by file corruption. For the older computers mouse deflection and screen effects were more routinely and consistently observed leading on to 'crashes' and latching of the software. A contributing factor to this could be that the modern computers tested have an electronic "soft start and shutdown" process controlled by the operating system. Older machines were more likely to feature mechanical on/off switches.

At no point during these experiments was permanent physical damage caused to the computers tested. For the Celeron computer temporary functional damage was experienced at several frequencies whereby it was necessary to re-install the operating environment (Windows NT) when an 'un-mountable boot volume' error occurred.

3.4.4.5 Standalone Computer – Extended Lower Frequency Bound

The opportunity arose to test one of the computers over an extended frequency range (100 MHz to 8 GHz). The brand D PIII 667 MHz computer was chosen since it would be the basis for the computer network susceptibility experiments. Figure 35 shows the susceptibility threshold of the PIII 667 MHz computer with the lower frequency bound extended down from 400 MHz to 100 MHz.

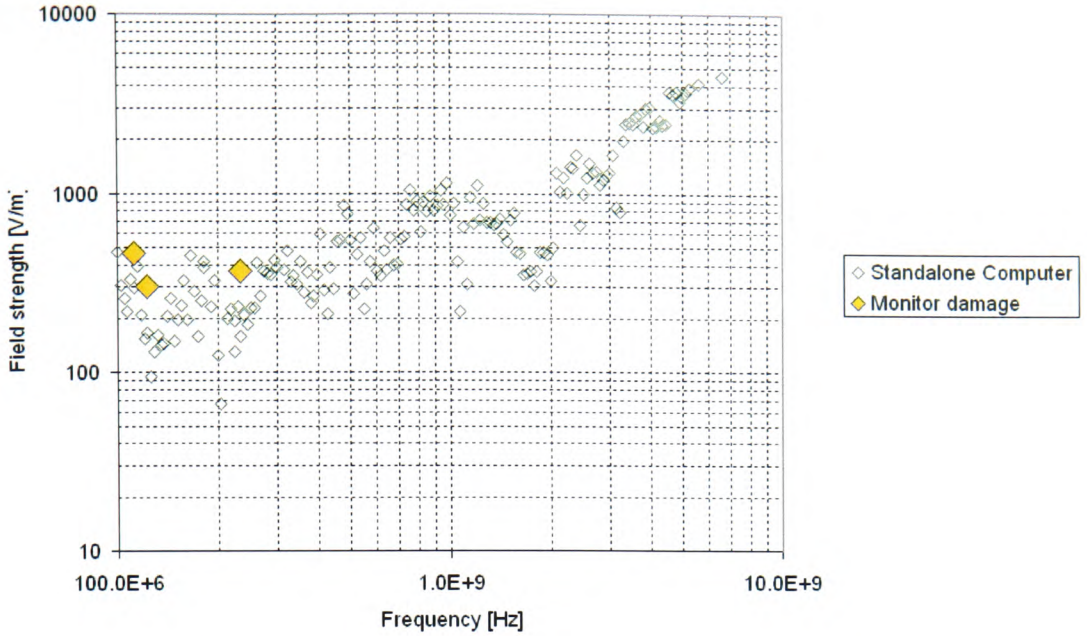


Figure 35: Susceptibility threshold of brand D PIII 667MHz computer (100 MHz to 8 GHz)

It can be seen that over this extended frequency range the susceptibility threshold has levelled out with a knee point somewhere between 500 MHz and 2 GHz. Also indicated are points where damage was found to occur, which was not previously observed. It was found that the 100 MHz to 400 MHz frequency range was extremely damaging for the computer monitors used as part of the SUT. In total three monitors were permanently damaged by the EM stress in this frequency range. The damage threshold and frequencies for the monitor failures is provided in the Table 26.

System Component	Frequency MHz	Peak field strength V/m
Monitor 1	112	470
Monitor 2	123	300
Monitor 3	234	370

Table 26: Monitor damage thresholds

The damage has not been investigated thoroughly but is symptomatic of monitor power supply failure. The monitor was changed to an LCD type which was found to be more robust over this frequency range so that testing could be resumed. It was found that the LCD monitor was generally more robust to EM disruption and that the monitor technology type had little bearing on the computer susceptibility threshold profile.

3.4.5 Summary of Standalone Computer Susceptibility Tests

The EM susceptibility of several computers with different specifications varying from 486 processor models to 2.6 GHz Celeron processor types have been evaluated. The

mode stirred (reverberation) technique was used with 3 % duty cycle pulse modulation. The test results show very good repeatability for susceptibility measurements of nominally identical computers.

The trend of the data shows that modern higher clock speed computers are less susceptible than their older counterparts across the frequency range tested (i.e. a higher magnitude is required to induce the same effect for the modern computers). This is counter to initial expectations since lower power and faster integrated circuits are being used in greater density in the higher specification more modern computers. It has also been shown that build quality has an impact on the susceptibility level.

Initially it was considered that the immunity threshold of the computers evaluated was different because of the introduction of the EMC directive. However, EMC directives concerning immunity have not changed significantly during the manufacturing period of the various computers tested, 1996 through to 2005.

It is certain that the internal clock frequencies of the computers are increasing. The actual clock speed specified by the manufacturer (66 MHz through to 2.6 GHz) refers to the internal processor clock speed. This is slightly misleading since there is very little transmission of the clock signal at these frequencies because the clock signal is confined to the processor chip die. Since the CPU clock is confined there is little opportunity for interfering with the clock signal and invoking a susceptibility. The main clock and the system bus frequencies are summarised in Table 27.

Processor Type	Processor clock frequency	Main clock frequency	System bus clock frequency
486DX	66MHz	33MHz	33MHz
PIII	664.51MHz	132.9MHz	132.9MHz
PIV	1.396GHz	100MHz	399MHz
Celeron	2.6GHz	260MHz	533MHz

Table 27: Computer clock specifications

It is generally accepted that the magnitude of the RF emissions will increase by 20dB per frequency decade increase and it can be seen from this table that there has been a decade frequency change in the clock frequencies that will contribute to RF emissions. It is clear from published materials that this has prompted computer system and processor manufacturers to find ways to control and minimise RF emissions to achieve EMC

compliance [Intel Xeon, 2000], [Intel P4, 2000]. Techniques that are used for the mitigation of computer emissions include:

- Dithered clock oscillators
- Differential clocking
- Multi-layer p.c.b. design
- Prevention of ground loops
- p.c.b. Edge stitching
- Finger-stock for enclosures
- Processor heatsinks
- Ground ring pads around p.c.b. vias (through holes)

Also of significance is the higher density of components on a single chip. In older machines the components would be distributed perhaps over several different p.c.b.'s and linked together. In newer computers with multi-layer p.c.b. technology the physical distribution of components is much lower and therefore they have shorter connections. This factor is likely to reduce the coupling efficiency of an external EM disturbance.

Effectively computer manufacturers are having to 'design in' EMC compliance in order to reduce circuit emissions that would likely disrupt their own circuitry and therefore system functions and causes them not to comply with EMC regulations. Since emissions of higher specification computers are actively being controlled by improved EMC design and because in simplistic terms the techniques for stopping RF getting out are the same as the techniques for stopping RF getting in. This appears to be improving the systems immunity (increased susceptibility threshold) via reciprocity.

The peak E field level required to produce a non trivial effect for a 2.6 GHz computer is almost an order of magnitude higher than the peak E field required for a 486 computer across the frequency range tested. An EM disruptor source with an operating frequency close to 2.4 GHz for example would need to produce a peak E field of 2 to 3 kV/m at a modern computer system to induce a significant effect compared with 300 V/m for the 486. Obviously this means that for the same EM disruptor source the effective range for a

modern computer system is less than that for an older computer system. This assumes that the optimum coupling angle is known.

However, it must be borne in mind that these discussions and assumptions are base on a very limited data set and much more susceptibility data must be gathered before statistically qualified trends can be established. It is also unclear whether the higher specification computers would be more susceptible than older specifications to other modulations and in particular narrow pulse width signals. It has been speculated that modern electronics may be able to respond more (increased susceptibility) to disruptive waveforms with narrow pulse widths and faster risetimes and therefore greater bandwidth [Watkins, 2005]. Very fast risetime (≈ 100 ps) and narrow pulses are typical of the Hyperband class of EM disruptors.

This series of experiments has highlighted some of the potential difficulties associated with the setting of an EM detection threshold.

3.5 Susceptibility Testing of Network Components

3.5.1 Aim

The aim of this series of experiments was to assess the EM susceptibility thresholds of wired (as apposed to wireless) computer networks and network components. Specific threats to wireless networks were discussed in Section 2.1.4.1 and fall outside of the scope of this thesis for the reasons discussed. Undoubtedly it is when computers become interconnected via networks that their usefulness is magnified they are also known to become more vulnerable.

To this end a series of susceptibility tests were performed using an iterative approach. In this way networking components were gradually added to a standalone computer to form a fully functional network. The objectives of this experiment were to:

- Compare networked computer and standalone computer susceptibilities
- Assess the types of effects induced
- Assess the impact on the user
- Identify critical components

3.5.2 System components evaluated

Several simple network configurations were developed and implemented. The range of System components tested included:

- Brand D PIII 667MHz computers with internal 10/100 MBps Ethernet cards
- A 10/100MBps PCI Combo network interface card
- A Dual Speed 10/100MBps switching Hub
- A 56kBps Modem router
- 2 x 20m Category 5 Shielded Twisted Pair (STP) Ethernet cables

A proprietary network analysis program called LanMarkPro was used to ascertain the EM effects on the network operation. Additionally the bespoke software programme discussed above (EMV software) was used to exercise each computer in the network to provide a constant level of CPU utilisation. LanMarkPro is a Transmission Control Protocol / User Datagram Protocol (TCP/UDP) packet generator and capture program with sophisticated control and management protocols and is designed for network performance testing. The software provides two pieces of raw data, Throughput, and Packet Error Rate (PER). A screen grab of the LanMarkPro user interface is shown in Figure 36.

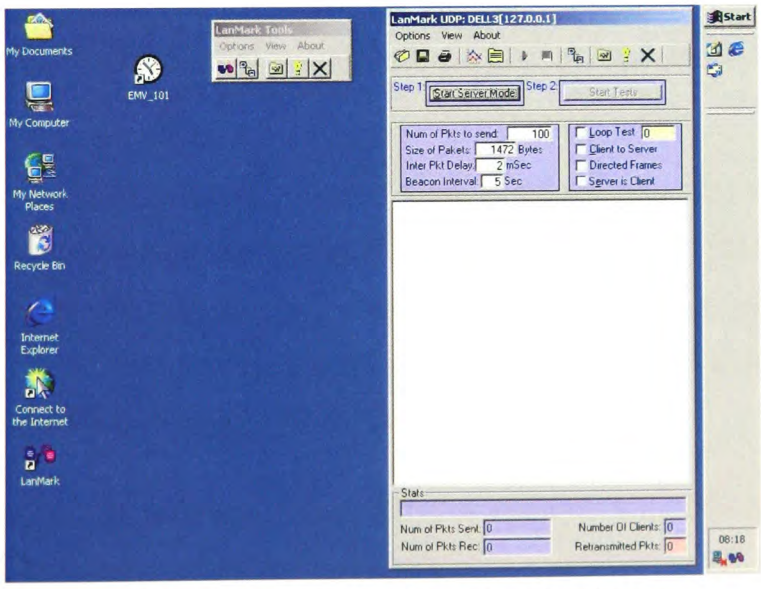


Figure 36: LanMarkPro software user interface

3.5.3 Test Configurations

The same reverberation chamber which was used for the earlier standalone computer susceptibility experiments was used for this test series. An advantage of the reverberation chamber over other techniques in this particular case is that the effect of cable layout is far less critical to the measured overall susceptibility threshold. A photograph of a networked computer within the reverberation chamber is given in Figure 37.

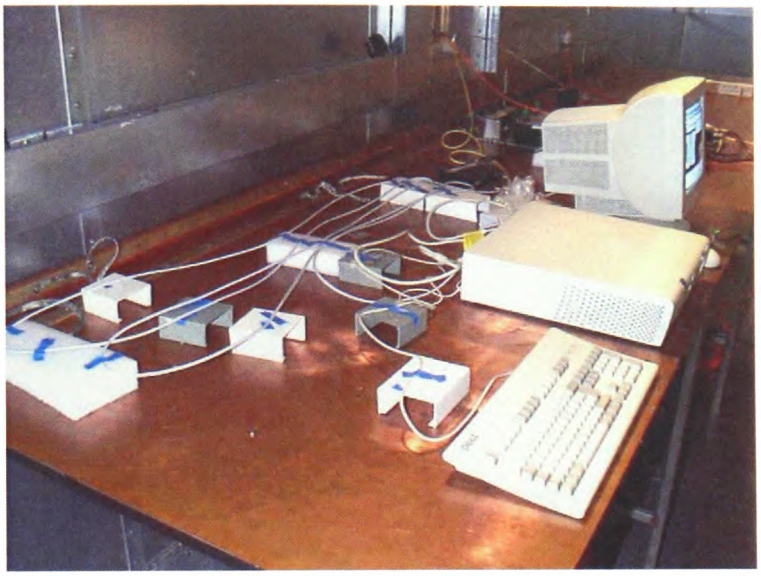


Figure 37: Networked computer in the reverberation chamber

The brand I PIV 1.4 GHz computer used in earlier experiments was used to generate and monitor network traffic from the control room annexe via fibre optic cable to the hub. In this way the network monitor was isolated from the EM disruption. An IEEE 802.3u 100-Base-FX Advanced Network interface card was used to facilitate the fibre optic network connection.

The frequency range for each test was 100 MHz to 8 GHz. The 400 MHz lower test frequency was extended down to 100 MHz for these experiments. This was necessary because the aggregated system was larger and therefore lower frequencies should couple more efficiently. 100 MHz was chosen because this was the practical lower frequency limit of the reverberation chamber used as discussed earlier.

The same 30 µs, 1 kHz (3% duty cycle) pulse modulation was used as in the earlier experiments allowing direct comparison of results.

3.5.4 Susceptibility Criteria / Observed Effects

As before for all tests the magnitude of the EM stress was gradually increased until the onset of an effect which required some manual intervention to re-set the status of the system. However, other effects specific to the network traffic were recorded:

- Network failures, i.e. Denial of Service (DoS)
- Temporary and permanent damage to components

Although the LanMarkPro software provided indicators of network (Throughput and PER) it was found that the indicators changed very swiftly from showing normal traffic to complete network failure. Therefore, no data on gradual network degradation was collected.

3.5.5 Observations and Test Results

3.5.5.1 Core Network Configuration

Figure 38 shows a representation of the system configuration for the first computer network experiment. Only the core system components of a hub switch and the necessary interconnecting cable between the hub and the computer have been introduced to the original standalone computer configuration.

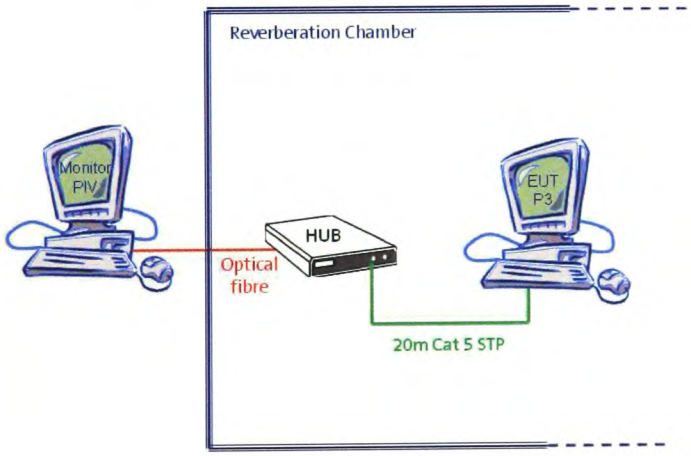


Figure 38: Core network configuration

For this test the network was exercised by sending packets from the control room computer via optical fibre. The network interconnection with the hub comprised of 20 metres of Category 5 STP cable. The first part of the experiment sought to evaluate whether the connection of the network cable affected the computer susceptibility

threshold. Figure 39 shows the difference in susceptibility threshold for exactly the same computer in networked and standalone configurations.

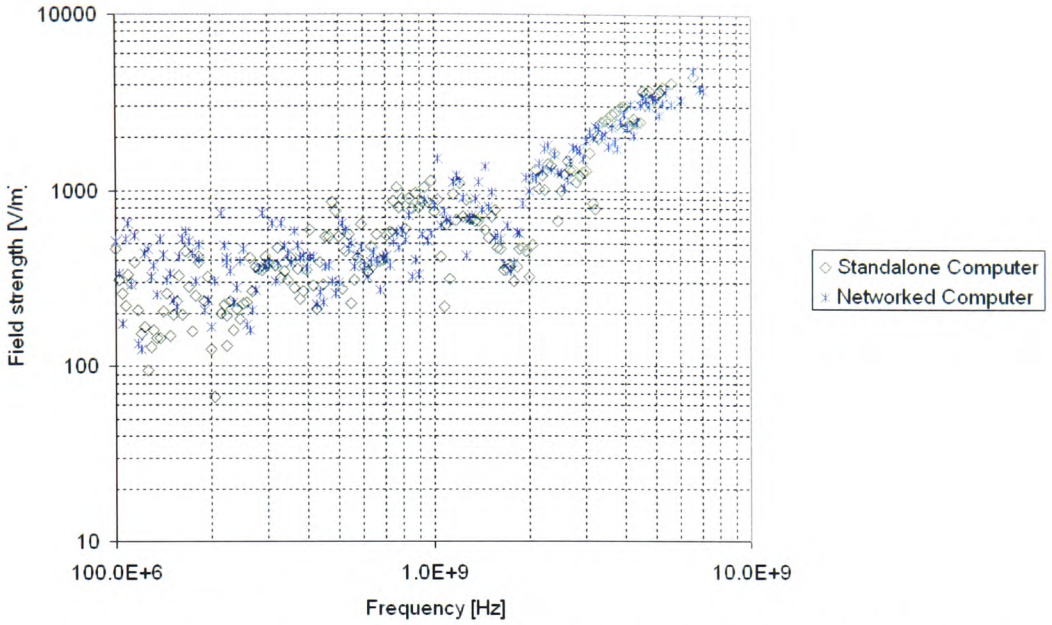


Figure 39: Standalone computer susceptibility threshold compared with exactly the same computer in a networked configuration

Interestingly it can be seen that there are only some minor differences in the susceptibility threshold for the networked and standalone computer configurations. This is further illustrated in Figure 40 where ±3dB error bars have been added to the stand alone computer susceptibility data.

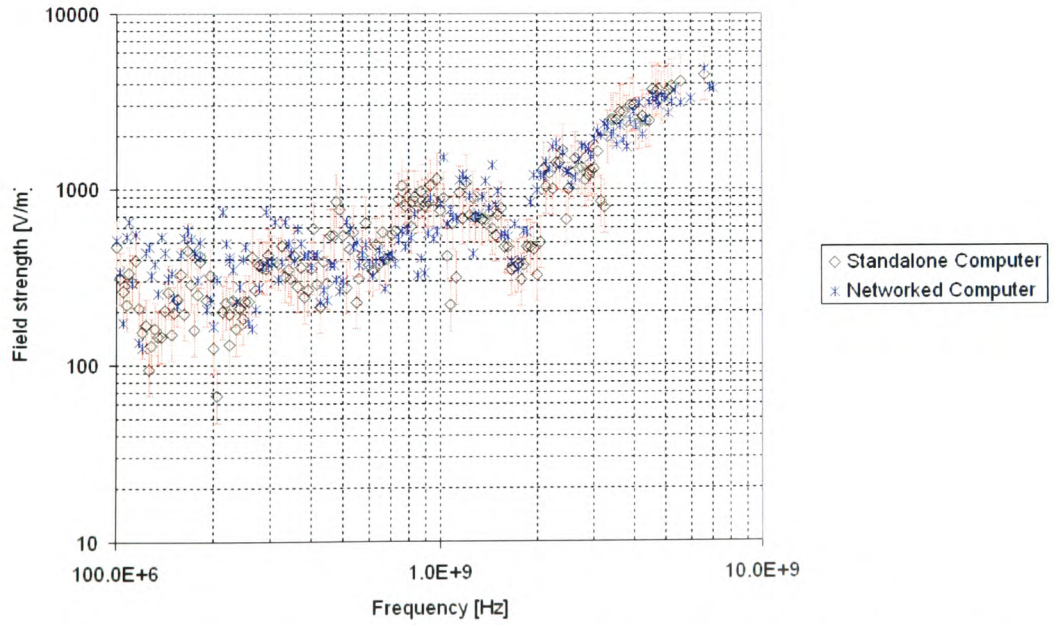


Figure 40: Standalone computer susceptibility threshold compared with exactly the same computer in a networked configuration, with error bars

Over certain frequency ranges illustrated in greater detail in the Figure 41, the standalone computer appears to be significantly more susceptible i.e. a lower field strength is required for the same effect.

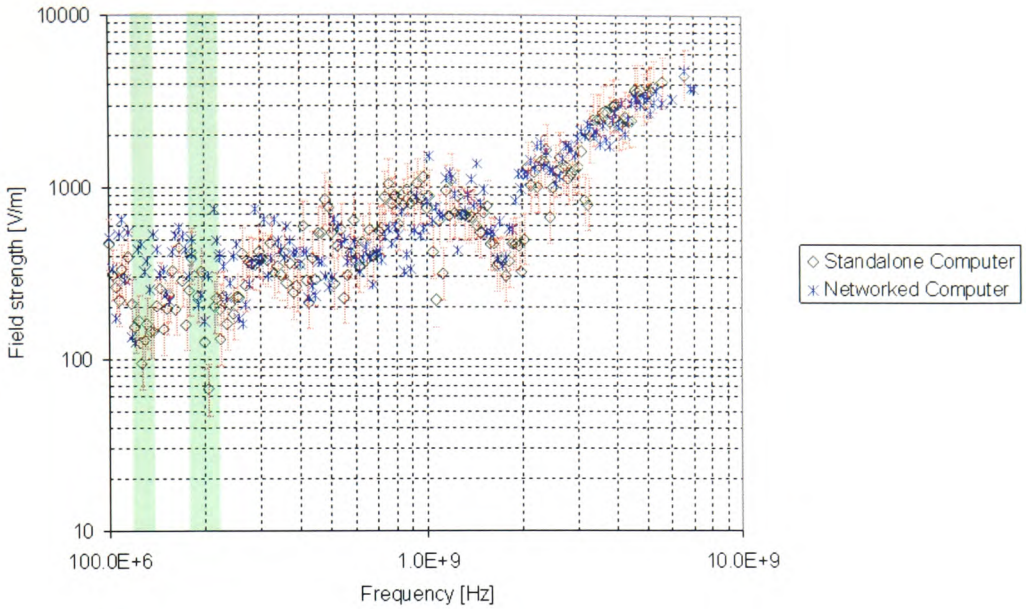


Figure 41: Standalone computer susceptibility threshold compared with exactly the same computer in a networked configuration with highlights

This result seems counter intuitive because at these frequencies one would expect the networked computer to be more susceptible due to longer cable lengths and therefore increased coupling efficiency. However, one possible explanation is that the network ports become electrically isolated or revert to a high impedance state when network failure (DoS) occurs. Since the port is isolated a path of EM ingress is removed thus reducing the occurrence of upset and increasing the susceptibility threshold.

The next stage of the experiment was to compare the susceptibility threshold levels at which the computer became affected compared with the susceptibility threshold levels when the network was degraded. As stated earlier network degradation was not gradual and proceeded from 100% packet transmission to 0% transmission (effectively DoS) with very minor increases in the EM stress. Figure 42 shows the networked computer susceptibility threshold compared with the network failure level (DoS).

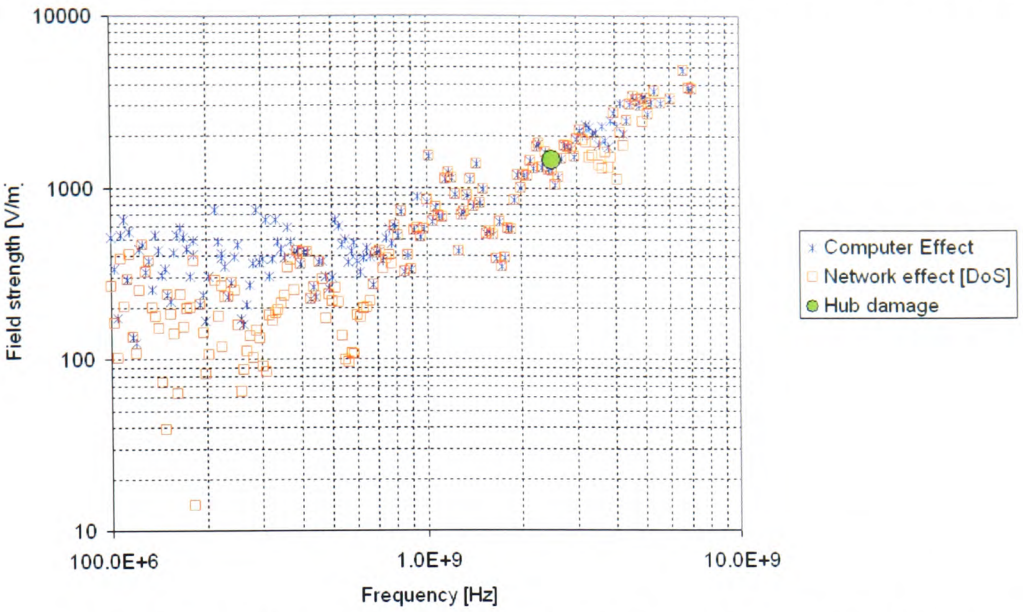


Figure 42: Comparison of computer susceptibility with network susceptibility (DoS)

It can be seen from the graph that there are strong regions where effects to the network (DoS) preceded effects to the computer (i.e. the susceptibility threshold to cause network DoS is lower than the susceptibility threshold of the computer). There are particularly strong regions where this effect is most pronounced these regions are highlighted in Figure 43.

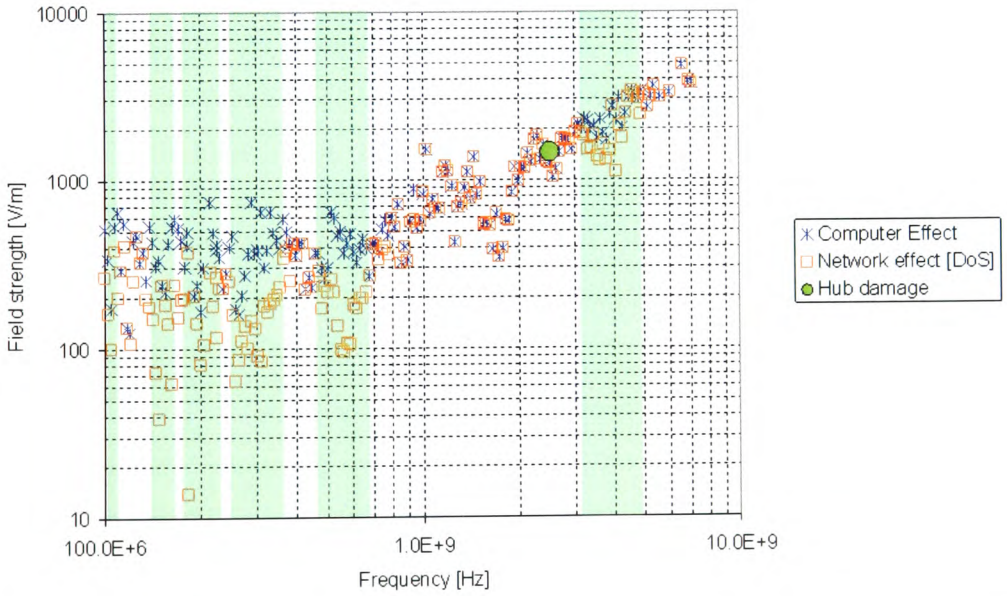


Figure 43: Comparison of computer susceptibility with network susceptibility - highlighted

In these regions the network outage preceded effects to the computer by a significant margin. The resonant peaks below 700 MHz are likely to be due to coupling to the network cable or network hub switch power supply cable. It was noted that in this region the network took a long time to recover. This perhaps indicates that the effect could be

due to thermal protection switching within the hub switch power supply. Increased susceptibility in the 3.16-4.26 GHz region indicates direct aperture coupling to either the hub unit or the hub power supply unit. The cable coupling region and hub aperture coupling regions are indicated in Figure 44.

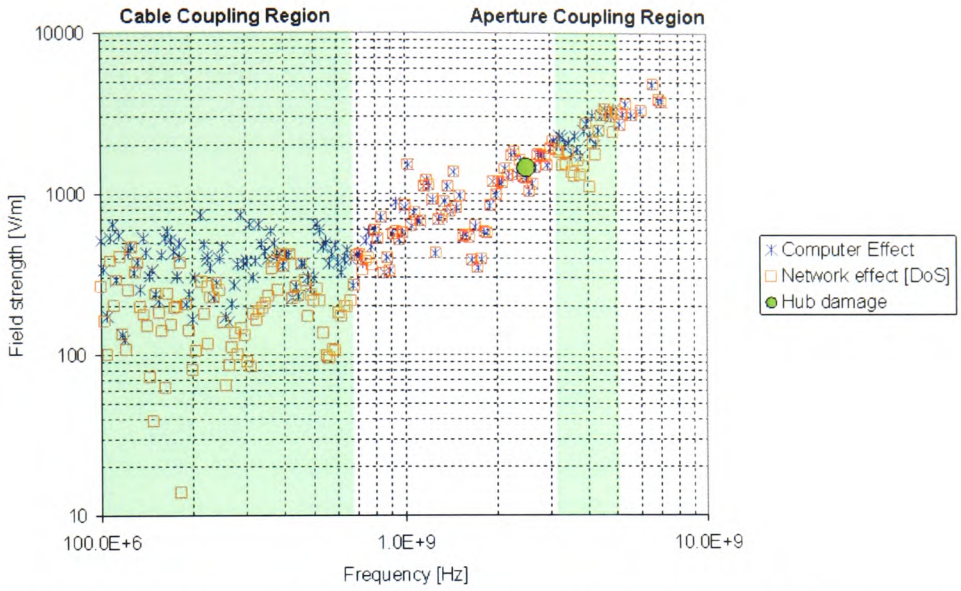


Figure 44: Comparison of computer susceptibility with network susceptibility (DoS) with predominant coupling regions highlighted

The hub or more correctly the hub power supply was damaged at 2.5 GHz with a peak field strength of 1.5 kV/m. Subsequent investigation revealed that the power supply was of a switched mode type. This type of supply is known to produce high levels of RF emissions and the evidence here suggests that they are also susceptible to EM disruption.

3.5.5.2 Small network configuration

Figure 45 shows a representation of the system configuration for a small network test configuration.

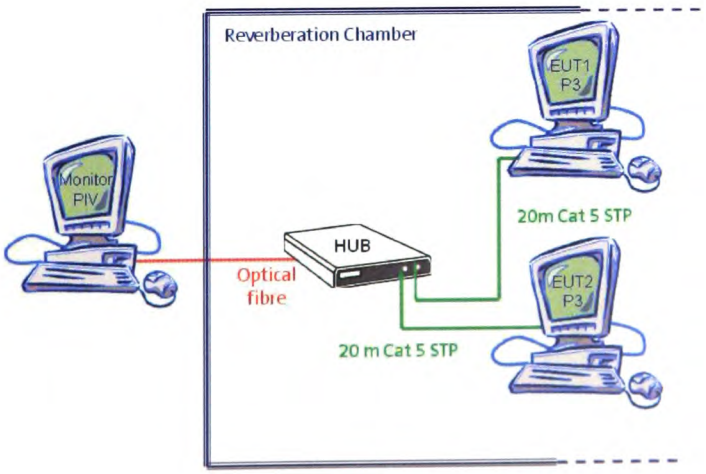


Figure 45: Small network configuration

For this experiment an extra computer was added to the network and exposed to EM disruption so that the iterative effect of larger numbers of computers in the network can be evaluated.

Figure 46 shows the susceptibility threshold for severe failure for EUT1 and EUT2 and the network failure (DoS) level.

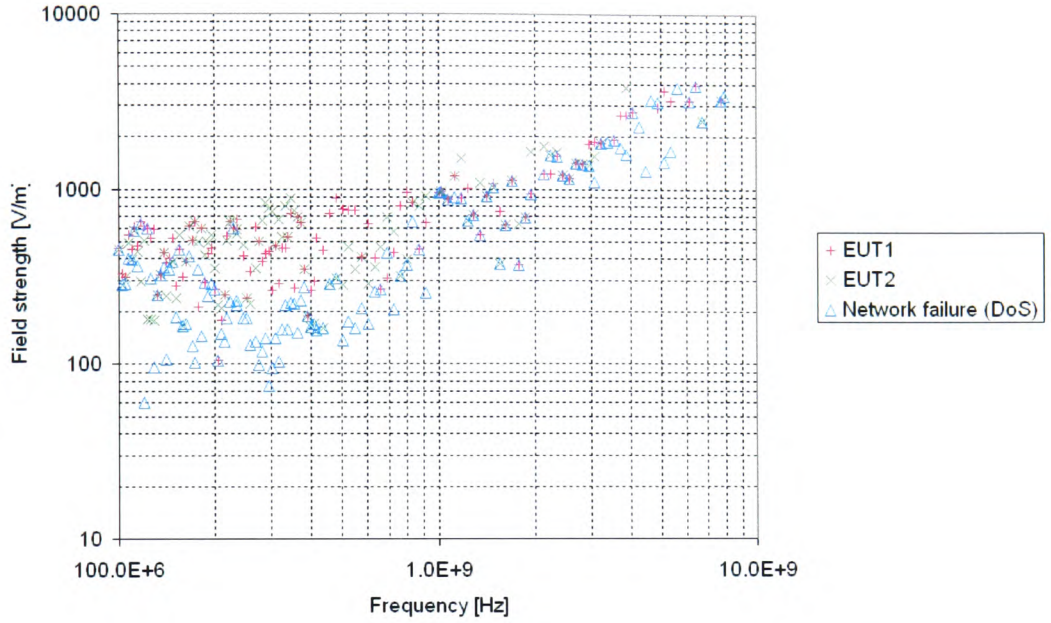


Figure 46: Comparison of DoS and computer susceptibility

As with the core network configuration there are regions where DoS is achieved at levels well below severe failure of the computer. These regions are illustrated in greater detail in the Figure 47.

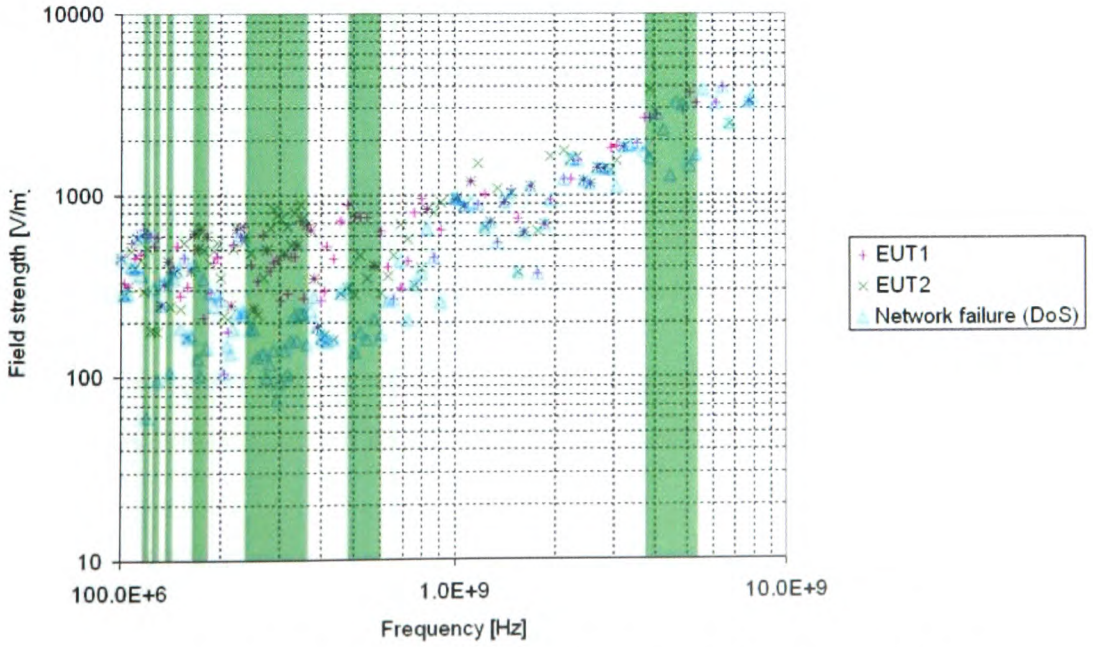


Figure 47: Comparison of DoS and computer susceptibility with highlights

In these regions the network outage preceded severe failure of the computer by a significant margin. These bands are similar but not identical to the core network configuration.

The susceptibility threshold for the two computers evaluated (EUT1 and EUT2) are fairly similar except for the region between 389-550 MHz where the susceptibility threshold for EUT2 is significantly lower. It is possible that due to the close proximity of the two computers within the chamber, one computer may have provided a degree of shielding to the other computer in this narrow region.

Figure 48 is a comparison between the DoS levels for the core computer network and the small network configuration.

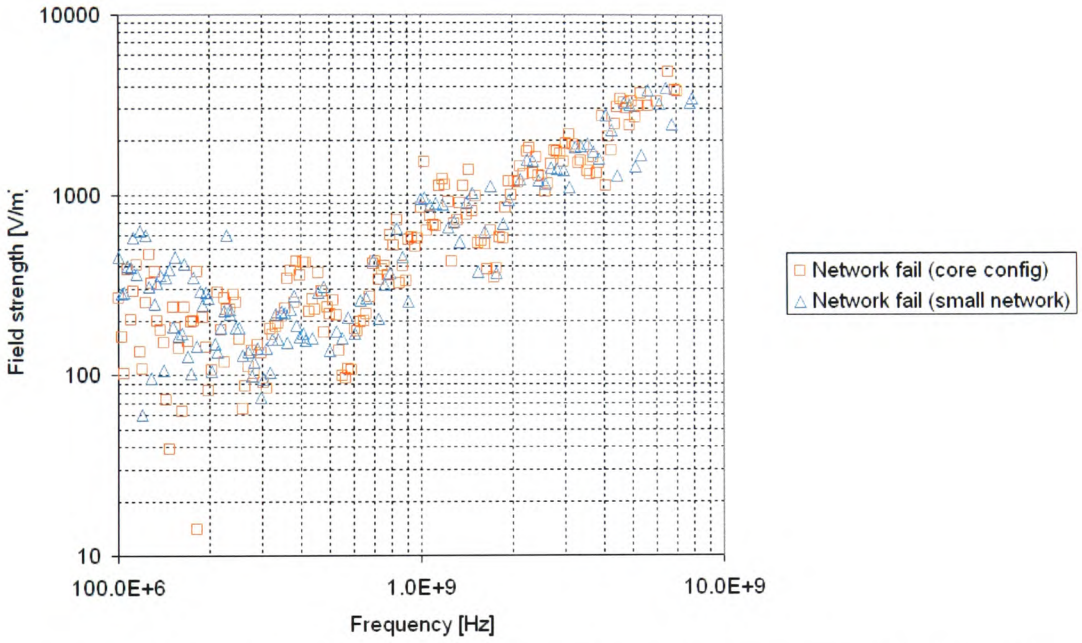


Figure 48: Comparison of DoS susceptibility threshold for the core network (1 EUT) vs. the small network configuration (2 EUT's)

It was observed that there were few differences in the susceptibility threshold for DoS but interestingly below 300 MHz the susceptibility threshold in key regions is higher for the small network case compared with the core network configuration.

Figure 49 shows the difference in susceptibility level for exactly the same computer when it is evaluated in standalone, core network and small network configurations.

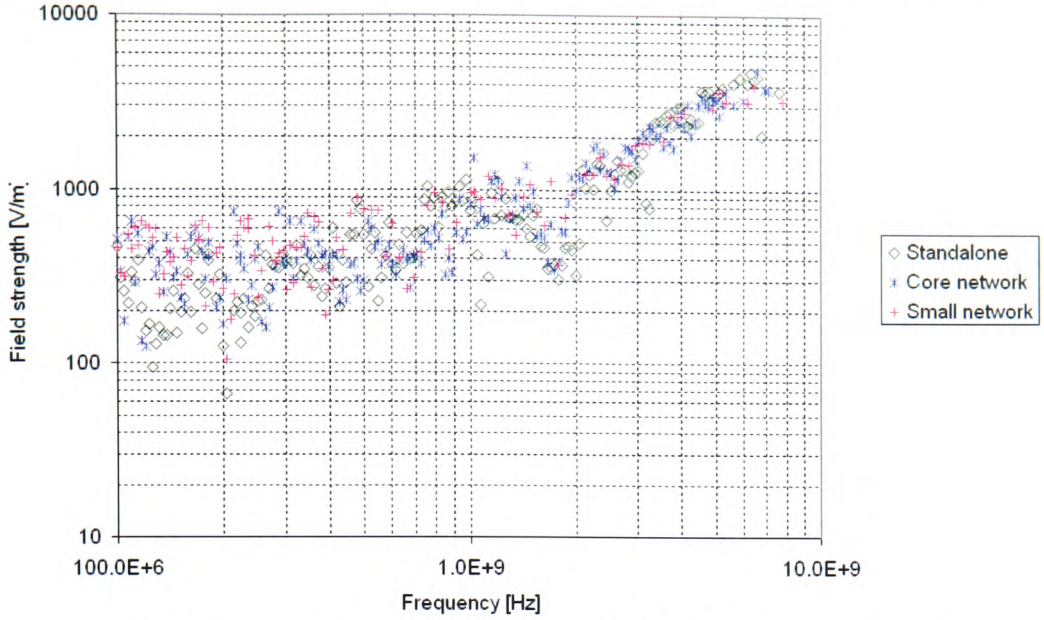


Figure 49: Comparison of the susceptibility thresholds for Standalone, core network and small network configurations

It was observed that there was little difference in the susceptibility threshold for the computer in each of the different configurations. This observation was similarly observed for the earlier comparison, Figure 41. At frequencies below 400 MHz it appears that there is a gradual shift in fact an increase in the susceptibility threshold as more systems are evaluated. This effect was also observed earlier. A possible explanation for this possible trend was provided earlier.

3.5.5.3 Wide Area Network (WAN) Configuration

Figure 50 shows a representation of the system configuration for this experiment.

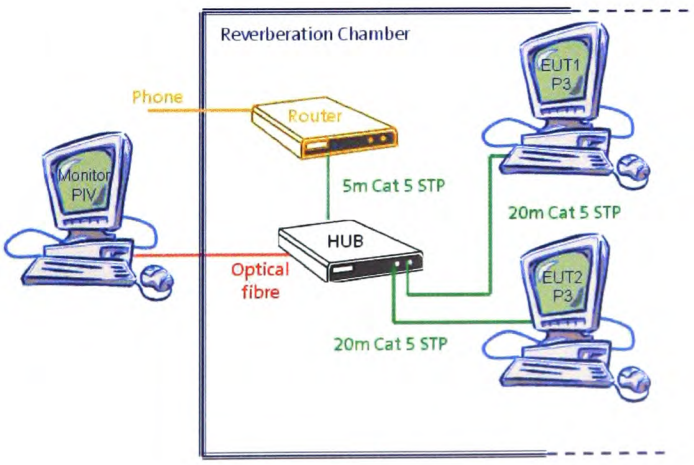


Figure 50: WAN configuration

For this experiment a router was added to the small network configuration. Unfortunately it was not possible to connect the router modem to a telephone socket completing the

WAN connection because it was not possible to guarantee effective EM isolation (i.e. the telephone line violated the reverberation chamber shielding). The router was exercised however, by 'pinging' the devices Internet Protocol (IP) address via the hub network connection. It is possible to speculate that the router would be more susceptible if the telephone connection was in place because telephone cable types are unshielded.

The lower frequency range for this test 100 MHz to 400 MHz was completed last due to amplifier availability issues. Figure 51 plots the susceptibility thresholds at which loss of the router connection, and computer susceptibilities occurred.

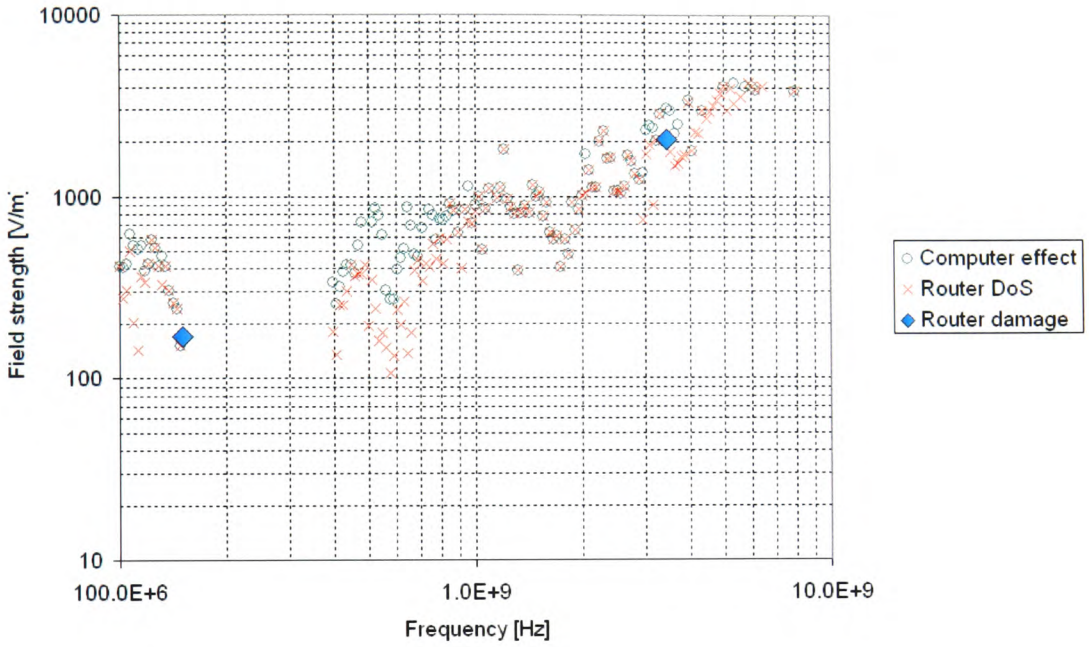


Figure 51: Router / network DoS compared with the computer susceptibility threshold

At two frequencies 151 MHz and 3.5 GHz router damage occurred. The nature of the damage was different in each case. For the damage which occurred at the higher frequency (3.5 GHz) the router was switched to a 'Test' mode and the status of the router was then fixed despite several attempts to reset the device. This probably indicates that the EM stress caused direct damage to the internal circuitry of the router. A new router was acquired and testing recommenced. For the damage which occurred at the lower frequency (151 MHz) the router failed to function completely none of the status indicators were illuminated. This probably indicates that the route of EM ingress was via the router power supply cable. The power supply in this case was a separate unit, but was a linear AC transformer type rather than a switched mode type as was the case with the hub. Further inspection revealed that the router external power supply unit was still functioning. It is therefore likely that internal voltage regulators within the router were

damaged. Another router was not available so testing was halted hence the absence of data between 151 MHz and 400 MHz.

As before there were regions where DoS was achieved at levels well below the susceptibility threshold of the computer. These regions are illustrated in greater detail in Figure 52.

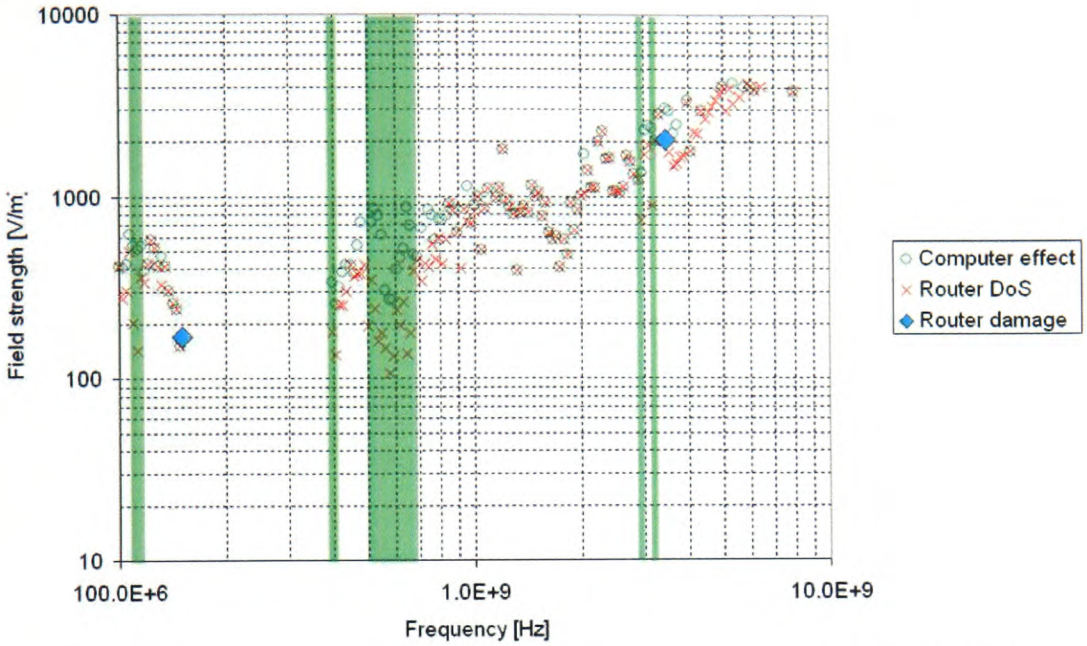


Figure 52: Router - network DoS compared with the computer susceptibility threshold with highlights

In these regions the router upset or network outage preceded effects to the computer by a significant margin. These bands are again similar but not identical to the small network configuration susceptibility test results.

3.5.6 Summary of Networked Computer Susceptibility Tests

A large range of effects were observed from network failure (DoS) through to permanent component damage.

It was found that in many cases DoS (loss of the network connection) occurred at lower total average E-field strengths than the onset of other severe effects to the computer under test in some cases by a significant margin.

This means that less stress was required to deny network service, than to severely disrupt the computers core function. In some instances the stress required for denial of service was an order of magnitude lower than that required to induce the preset susceptibility criterion of the computer. The manifestation of the network failure appeared as a swift

transition from a satisfactory network connection to complete network failure. Gradual degradation was not observed.

Once service was denied it was not possible to restart the network connection with the EM stress present. Once the EM stress was removed it was possible to re-initiate network traffic but only from the control computer terminal. This factor is significant since remote restarting of the network was not possible.

The cause of the network failures was most likely due to coupling to the peripheral network components (hub and router) via the power supply cable, the network cable and the peripheral enclosures. In particular the power supplies were found to be prone to damage. From a brief visual investigation the construction of the network components seemed less well engineered than the computer construction.

The tests above were conducted on a fairly robust system since Ethernet category 5 STP (shielded) cable was used in preference to unshielded types and the unshielded telephone cable for the router was left unconnected. It is speculated that Unshielded Twisted Pair (UTP) Ethernet category 5 cable (or lower categories) are likely to lower the susceptibility threshold for DoS further since the cable coupling efficiency will be higher.

It is important to realise that the network components (hub and router) and computer network interface card may not support STP (i.e. Shielded sockets must be specified during acquisition). In some instances it may look as if the cable socket is metallic but this does not guarantee that the shield is maintained to the enclosure of the network component. Without an STP compatible socket the use of STP cable will probably not provide any additional protection. The benefit provided by STP is only valid if the shield is maintained end to end [Bell, 2004].

Interestingly there were no major differences in susceptibilities for the computers themselves in any of the network configurations. It was expected that a network configured computer would perhaps be more susceptible because the extra cable lengths would mean that the coupling efficiency was higher. However, the data shows that the differences are minimal.

For the core computer the network connection does not make the computer more susceptible (i.e. lower the susceptibility threshold). However, for a directed plane wave threat, (i.e. the types of threat likely to be produced by a mobile EM disruptor) a

distributed network of computers has more chance of being affected because of the enhanced possibility of coupling stress to some point in the network. This is an important finding which highlights the value of these tests.

Some key features of the network susceptibility tests are tabulated in Table 28.

Frequency	Effect
148MHz	DoS occurs at lower EM stress than computer latch up or shutdown
155MHz	DoS occurs at lower EM stress than computer latch up or shutdown
182MHz	DoS occurs at lower EM stress than computer latch up or shutdown
300MHz	DoS occurs at lower EM stress than computer latch up or shutdown
550MHz	DoS occurs at lower EM stress than computer latch up or shutdown
2.5GHz	Hub damage
3.8GHz	DoS occurs at lower EM stress than computer latch up or shutdown
Other frequencies	Computer latch up or shutdown occurs At the same time as DoS

Table 28: Key features of the network susceptibility test

3.6 Comparison of Susceptibility Results with Published Data

It is perhaps important to understand how these susceptibility results compare with the results discussed in Stage I, Section 2.5. A rough comparison can be achieved by comparing the data from the Stage II, Section 3.4.4.4 tests above with the published data. However, the modulation type used within this series of experiments is again different to the modulation types used for the effects data found in the literature. Nevertheless a crude comparison can be made in terms of the average power density as per the previous approach.

Figure 53 shows the data from Figure 33 together with the published data set.

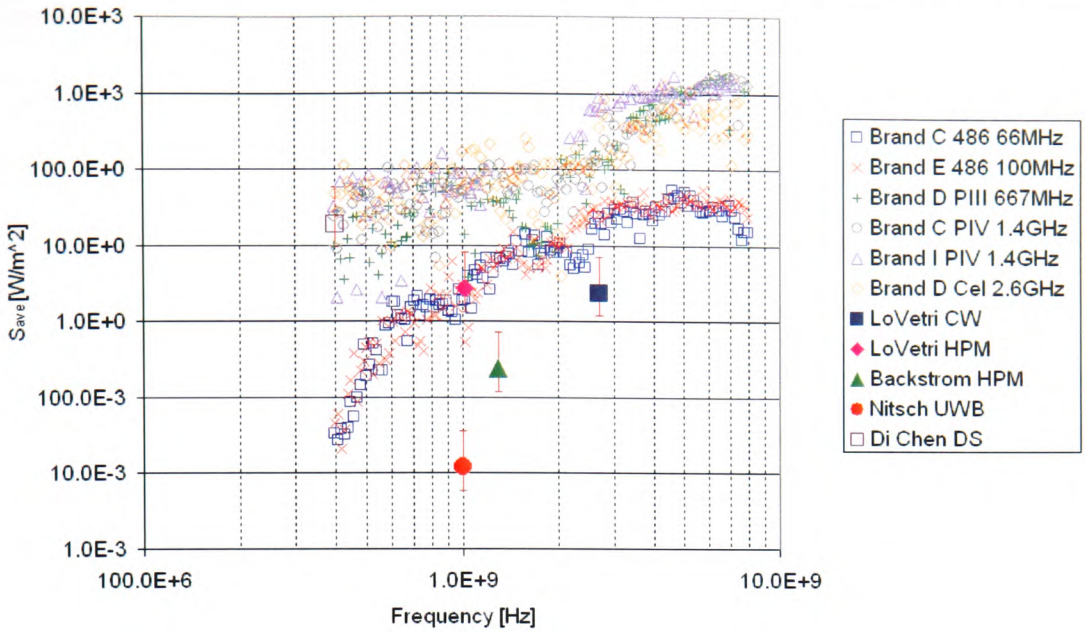


Figure 53: Susceptibility data in terms of effective power density

It can be seen from the graph that in general the average power density values for the published data are lower than that observed from the experimental susceptibility test campaign conducted as part of this study. However, comparison is difficult since many factors regarding the test configuration from the published data are not provided. For example the Backstrom data [Backstrom, 2004] is an extrapolation and no details of the computer system tested are provided. The LoVetri data [LoVetri, 1999] for the HPM (Hypoband) waveform compares fairly favourably with our experimental data whereas the LoVetri CW data appears to be an order of magnitude lower than this experimental data.

The Nitsch UWB (Hyperband) test data [Nitsch, 2005] appears to demonstrate that the bandwidth of the signal (which is related to the pulse rise time and pulse width) could have an impact on the average power density required at the target computer system.

For the reasons discussed above and those discussed in Sections 2.3.3.2, 2.3.3.2.1 and 2.4.3 of this thesis it can be seen that the definition of a susceptibility threshold is extremely complex and is dependent upon many factors principally:

- The general inaccuracy or uncertainty associated with the other test methods
- The test conditions (illumination angle, SUT layout, calibration, measurement of the peak E-field, shot to shot variation, test repeatability)
- The EUT type and specification

- The instantaneous bandwidth of the disruptor waveform

These factors amongst others lead to extreme difficulty in assigning a truly deterministic susceptibility comparison metric to the data.

It has been shown however that reverberation chamber testing undertaken in this experiment provides a solid foundation given that the test conditions are more rigorously controlled with a degree of statistical averaging inherent in the test technique.

For the reasons discussed above, the reverberation chamber experimental susceptibility data taken here will be used for further analysis and development of EM detection concepts.

3.7 Observations of Audit data with respect to Susceptibility

Throughout the computer susceptibility experimental campaign the event log files were examined using Windows Event Viewer and the network Throughput and PER was examined using LanMarkPro. Given the variety of effects observed during effects testing as shown in Table 25 it is surprising that very little relevant information was found. It has already been stated that gradual network degradation was not recorded and that the onset of network failure was rapid.

The only relevant information obtained form the event viewer log files throughout the test campaign pertained to mouse deflection and upset. The event log window is shown in Figure 54.

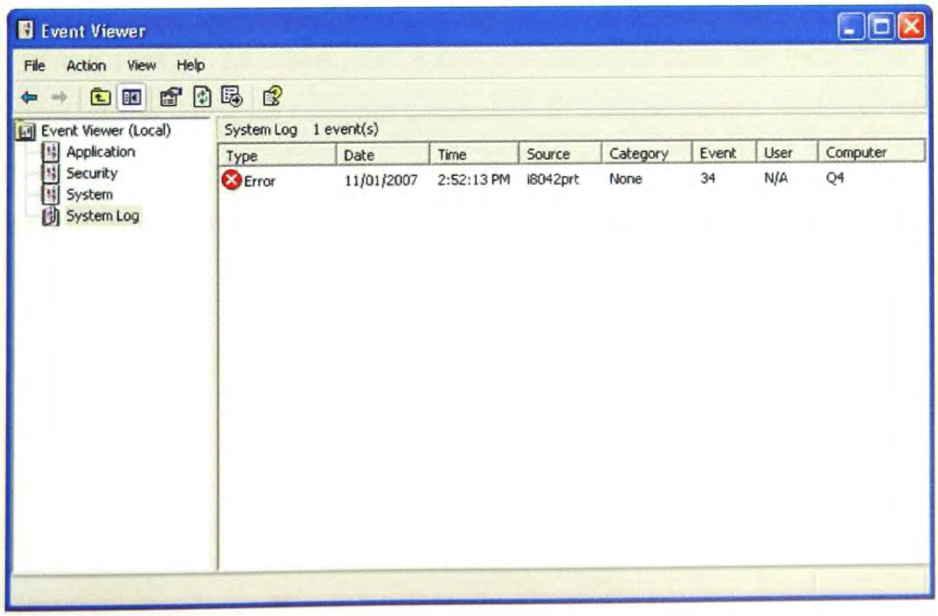


Figure 54: Event Viewer window after thorough susceptibility testing

This error message corresponds to mouse pointer deflection, mouse button operation and intermittent slowing of the EMV test software. The error source code i8042 corresponds to the ps/2 keyboard and mouse port on the personal computer.

No event logs were created for any of the other susceptibilities observed including network susceptibilities. Clearly, then event log files and possibly other audit processes, on there own cannot be relied upon to provide indication of susceptibility.

3.8 Stage II – Summary

This series of experiments has principally demonstrated:

- The usefulness of the reverberation chamber susceptibility test technique
- That computer systems and computer networks are susceptible to EM disruption
- That two very broad classes of failure can be observed upset and damage although damage was only observed for peripheral components
- The variety and complexity of effects observed
- The complexity of susceptibility data
- The trend with increasing computer susceptibility threshold with improving computer specification
- The potential differences between cyber DoS and EM disruptor induced DoS

The *functional* aspects i.e. how the hardware will actually be used has not been considered as part of this experimental campaign. It is important to note that many types of functional disruption may exist and this will add another dimension to the uncertainties associated with susceptibility determination.

Consider the impact of EM induced DoS since it has been found that it was necessary to re-cycle the power on the hub switch or router this could have variable consequences depending on the network function. For a small central office the network administrator is likely to be in close proximity to the susceptible device allowing for fast re-instatement of network functions. However, there are many scenarios where the susceptible system may be inaccessible or at least remote from the administrator for example a remote terminal unit which is part of a distributed control system controlling a water pump gate

valve. For these scenarios where the network cannot be remotely initialised the functional impact could be far greater in the above example large areas could be flooded.

Given this data and the speculation about the functional issues it is clear that ITE systems and therefore information process and information availability are susceptible to EM disruptor action. Further, since traditional techniques such as examination of event logs and monitors do not provide indication of susceptibility to EM disruption, the utility of detecting EM disruption must be explored.

The data produced through this experimental campaign provides an excellent grounding for the development of an EM disruption detection system and assists in the formulation of an EM disruption detection threshold.

4 Stage III – EM Attack Detection and Incident Response

4.1 Aims and Objectives

The aim of the third and final stage is to develop concepts for EM detection and to develop one of the concepts into a proof of principle demonstrator.

Objectives:

- Develop detection concepts based on conventional threats to INFOSEC
- To take at least one these concepts through to a proof of principle experiment stage
- To promote a synergy of understanding between conventional and EM threats
- To postulate how EM detection can be used for forensics and incident response

4.2 Cyber Intrusion Detection Systems

The purpose of this section is to provide a brief review of the application and utility of computer Intrusion Detection Systems (IDS) and to subsequently use this knowledge to

derive desirable features for EM detection and diagnostic systems. An overarching aim is to produce a specification for an EM detector which is compatible with modern cyber IDS. Only those aspects of IDS considered to be most relevant to EM disruption detection are discussed.

4.2.1 The Function of IDS

IDS are often compared with sophisticated burglar alarms [Rozenblum, 2001]. They can detect threats to computer systems as they occur rather like the Passive Infra Red sensor linked to an outside security light can detect the proximity of an intruder. Further, once an intrusion has occurred they can subsequently be used to provide evidence of exactly how the intrusion was carried out and what was stolen or adversely affected but most importantly they alert to the fact that a threat is being perpetrated. In the instance of a burglar, and in some instances for cyber threats, this alert may be sufficient to warn off the perpetrator or provide sufficient time to allow protection measures to be enacted.

At the very least the IDS alerts the user to the fact that a susceptibility has been exploited. Vulnerabilities are therefore identified and countermeasures can thus be implemented. For cyber type threats this process is generally achieved by downloading a patch for the firewall and an update for the IDS malicious behaviour library for the new form of threat. This repair protects the system from the next occurrence of the same threat.

Another analogy compares IDS systems with a firewall in a military scenario thus a firewall is compared with a soldiers helmet and flak jacket whereas an IDS is compared with the medic who provides first aid. It is clear then that IDS systems play a vital but not totally comprehensive role in the maintenance of INFOSEC.

4.2.2 Intrusion detection design

Many authors in the field of cyber intrusion detection [Proctor, 2001], [Bruneau, 2001] cite the works of Anderson [Anderson, 1980] and Denning [Denning, 1987] as the seminal treatise on cyber intrusion detection.

The requirement for intrusion detection seems to have emerged from an 'increasing awareness' of computer security problems for the US Air Force (USAF) especially when they began to share different levels of classified information over rudimentary computer networks.

The initial IDS design approach attempted to analyse accounting audit files in order to detect unauthorised access. This audit process remains as the cornerstone of many modern IDS. However, the biggest problem and one that remains to this day was how to differentiate between authorised and unauthorised access and subsequently how to define threat types and characteristics (behaviour analysis).

Denning's intrusion detection model lead to the development of real-time intrusion-detection expert systems that aim to detect:

'a wide range of security violations ranging from attempted break-ins by outsiders to system penetrations and abuses by insiders.'

The model is based on the hypothesis that exploitation of systems vulnerabilities involves *abnormal use* and that detection of abnormal behavioural patterns is the key for detecting threats. The sorts of threat behaviour considered in the model include:

- Attempted break-in
- Masquerading or successful break-in
- Penetration by legitimate user
- Leakage by legitimate user
- Inference by legitimate user
- Trojan horse
- Virus
- Denial of Service

Some of these behaviours could be non-malicious and even accidental. The model, which is essentially a rule based pattern matching algorithm, is designed to be completely generic and independent of specific system architectures and vulnerabilities. In essence the concept is to monitor standard operations on a computer system such as:

- Log in attempts
- Command execution

- Program execution
- File access
- Device access
- Network traffic

The IDS must therefore compare standard patterns of behaviour against suspicious behaviours such as deviations in standard usage. In essence the basic IDS model assesses the interactions between subjects and objects and uses rules, profiles and records to indicate anomalous behaviour. This model is fundamentally the same as that used for modern day IDS. The sorts of processes enacted by modern IDS are:

- Monitoring and analysing user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Statistical analysis of activity patterns based on the matching to known attacks
- Abnormal activity analysis
- Operating system audit

4.2.3 Implementation

IDS can be described as host based and network IDS. The essential difference between these two types of IDS is that host based systems analyse activity on the computer core system such as file access, application execution etc. Network based IDS analyse the traffic on the network. For network IDS there is further sub categorisation these are known as promiscuous mode network IDS and distributed or network node IDS. Both types deploy 'sensors' which 'sniff' packets on the network with the aim of detecting abnormal behaviour. However, network node IDS only sniff those packets bound for a single destination computer which is likely to be a node having some critical function.

A block diagram of a typical Network intrusion detection system [Proctor, 2001] is shown in Figure 55.

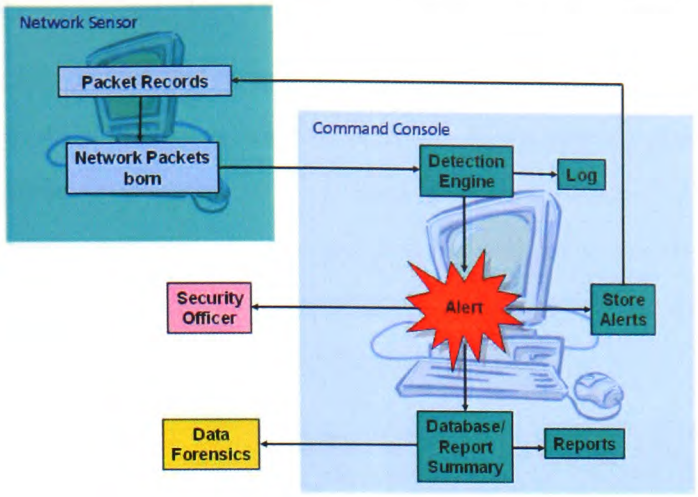


Figure 55: Typical Network IDS configuration/function

The network sensor in this Figure can be software based running on an appropriate host or a hardware implementation such as a router.

4.2.4 Problems Associated with IDS

One of the biggest problems with IDS is in differentiating between truly malicious or unacceptable behaviour and accidental or acceptable behaviour. Any alarm type system quickly loses credibility if too many false alarms are produced [Northcutt, 2003]. Four outcomes are considered possible from IDS systems which can be described by the following diagram, Figure 56.

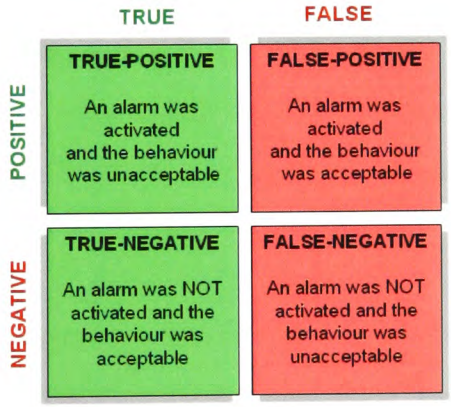


Figure 56: True/false negative/positive diagram

False-positives are seen to be the most problematic because alarms require analysis and therefore a false alarm requires nugatory activity which has an inherent time penalty which may slow down processing functions. False-negative alarms are perhaps the most serious since unacceptable behaviour was allowed and not detected. However, false-positives are the most likely to cause degradation of user confidence of an IDS system.

4.2.5 Summary

IDS provide an essential INFOSEC function by alerting to the fact that unacceptable or undesirable behaviour is taking or has taken place. Since many cyber type threats can manifest in very subtle ways some form of alarm system is essential. Once an alarm has been raised recovery or repair strategies and even preventative action for the next time the threat occurs can be put in place. The utility of detection/indication in an INFOSEC context can be explained via the following diagram, Figure 57.

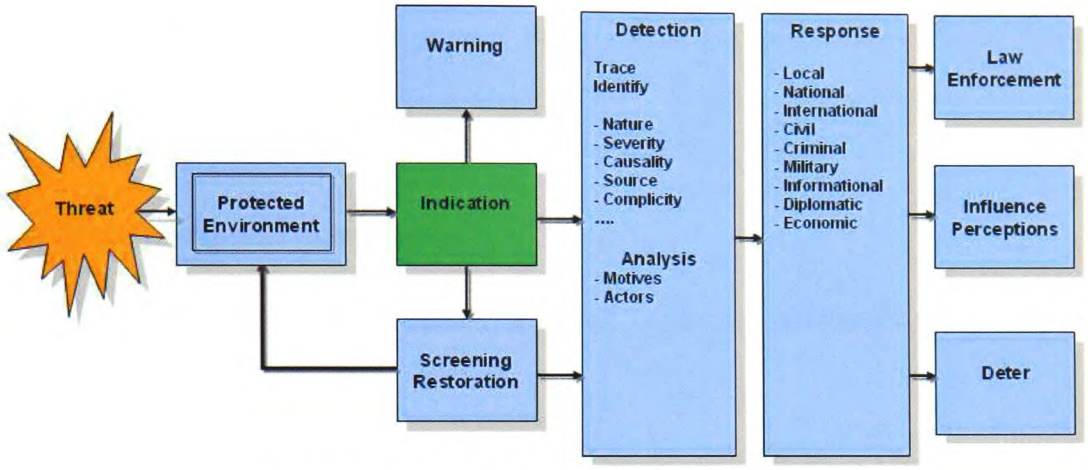


Figure 57: Utility of detection for understanding INFOSEC risks

It has been discussed earlier that EM disruptive threats have some similar characteristics with cyber/CNA type threats and in particular DoS. Given that the traditional IDS approach of detecting abnormal behaviour through audit processes is not applicable to EM disruptive threats (see Section 3.7) it is clear that detection/indication of EM disruptive threats may be a very useful step in understanding the risks posed to INFOSEC from EM threats. Therefore, the feasibility of providing EM disruptor threat detection will be addressed.

4.3 EM Disruptor Detection System (EMDDS) Development

It is clear from the above discussions that computer systems and network system components are susceptible to EM disruption and it is also clear that effective countermeasures/mitigation exists. However, the crux of the matter is that potentially costly mitigation measures will not be employed if those responsible for implementing INFOSEC do not believe that the risk from EM disruption is real or at least of a sufficient magnitude to warrant action.

The aim of this section is to develop a specification of an EM Disruption Detection System (EMDDS). The primary function that this system will fulfil is detection,

indication and alerting of the fact that the source of computer system malfunction is EM in origin. A secondary function is for the detector to provide evidence that can be tested by forensic scrutiny. Once this indication has been provided other stages such as recovery, analysis and response can be enacted.

The objectives are therefore, to:

- Identify a set of desirable and essential requirements of an EMDDS
- Create a set of detection system specification parameters based upon known threats and the susceptibility data gathered through the experiments discussed in Stage II
- Identify candidate technologies
- Summarise the technical issues involved with the development of detection systems
- To take at least one detection system concept through to a proof of principle experiment stage

4.3.1 EMDDS Requirements

Drawing upon the discussion concerning cyber IDS above, Table 29 has been developed which describes requirements/desirable features of an EMDDS.

Requirement Number	Essential/ Desirable	Description
R1	Essential	The manifestation of EM disruption and the actual disruption mechanism are not well known, extremely variable and imbued with high uncertainty. Analysis of the computer function alone (e.g. through audit processes using traditional IDS) is not sufficient. The EMDDS must incorporate an EM sensor to sense the EM stress
R2	Essential	From published susceptibility data the frequency response of the EM sensor must cover the frequency range from 1 MHz to 10 GHz and be able to sense very narrow impulsive waveforms (such as UWB with rise times of the order 100 ps and pulse widths down to 200 ps). The frequency range from 1 MHz to 100 MHz is best detected with a cable sensor which detects coupled stress. The frequency range from 100 MHz to 10 GHz is best detected by a radiated stress sensor
R3	Essential	The sensor must be capable of detecting EM stress levels with magnitudes below the onset of upset through to damage. This corresponds to an amplitude dynamic range of approximately 50dB given published evidence
R4	Essential	Since a perpetrator is likely to use an EM stress level significantly above the threshold required for disruption to guarantee success, the sensing element and any event logging hardware or command console must be extremely robust to the EM stress or at least provide indication of failure
R5	Desirable	The EM sensing element of the detector must be sensitive to EM disruption from any direction i.e. the primary sensing element must be omni-directional
R6	Desirable	Providing an indication of the location (direction finding) of the EM disruptor source would be a very useful feature
R7	Desirable	The EM detection system should provide detailed information on the characteristics (frequency, magnitude, pulse parameters, etc.) of any identified disruptor waveforms. The disruptor types should also be logged
R8	Desirable	The system should be compact, self-contained, low maintenance and offer long-term operation independent from power sources which may be affected by EM disruption i.e. battery powered.
R9	Essential	The cost of employing detection is a very important factor and must at least be less than the cost of mitigation. Studies have shown that the cost of mitigating EM disruption depends on the stage of the system design process in which it is considered. Shielding a small facility with a volume of $1000m^3$ is expected to cost £120,000 using inflation adjusted 1991 figures [ETL91-2, 1991] A target maximum cost for supply of the EMDDS of 5% of the cost of shielding (i.e. £6,000) is considered reasonable expenditure for a facility
R10	Desirable	EM disruptor detection based only on sensing EM stress has no false positive since EM threshold detection indicates that the threat is of a sufficient magnitude to produce alarms (the origin of the disruption could be malicious or non malicious, intentional or un-intentional). However, it may be difficult to justify alarms based on EM stress only if no disruption to the information process was encountered. A detection mechanism which correlates the EM stress level with information process malfunction is clearly the most robust detection mechanism with the lowest false alarm rate
R11	Desirable	The EM detector should be able to seamlessly integrate with conventional IDS and be understandable to non EM specialists
R12	Desirable	The detection system should detect EM disruption before the susceptibility impacts on the function of the system or process. However, this could potentially lead to a greater number of false alarms (see R10)
R13	Desirable	For application to expedient incident response and to facilitate successful criminal prosecutions the EMDDS should time and date stamp any alarm and this data should be stored in non-volatile memory and be capable of being authenticated, thus providing forensic evidence

Table 29: Technical and Functional Requirements of the EMDDS

Some of the elements are subjective and based upon reasonable estimates based on interpretation of available data. Requirements (R1), (R2), (R3), (R4), and (R9) are

considered essential for the EMDDS concept prototype. The remaining requirements identified are considered desirable but not essential for the initial prototype.

A block diagram of the potential functional structure of the EMDDS is given in Figure 58.

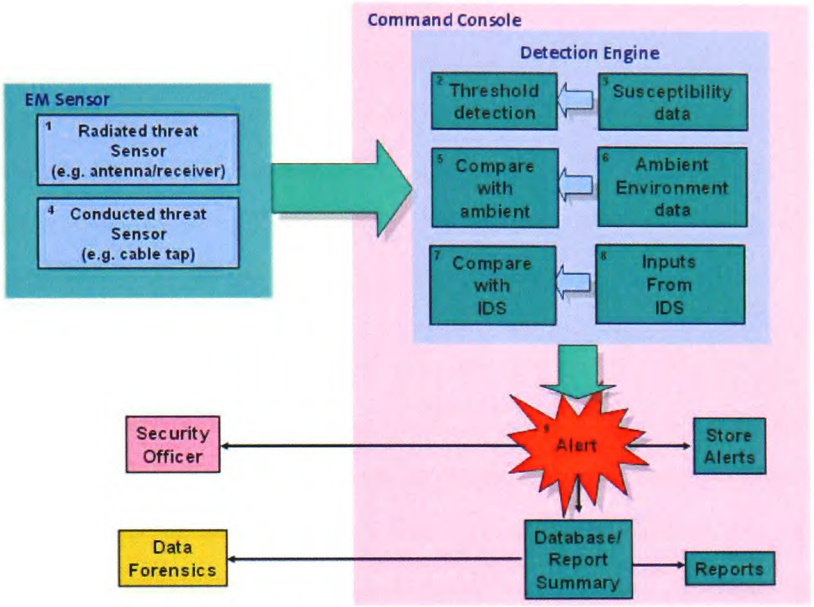


Figure 58: Functional structure of an EMDDS

The relevance and importance of each of the functional elements can be described thus:

4.3.1.1 The EM Sensor

The EM sensor comprises two elements a radiated threat sensor [(1)] and a conducted threat sensor [(4)]. The purpose of the radiated threat sensor is to respond to the EM field impinging on the victim/receptor system. The purpose of the conducted threat sensor is to respond to transients injected on cables or conductors, or to respond to transients induced in cables or conductors from radiated fields which are attached to the victim system. In some instances it could be useful that the two sensors are used to correlate with each other reducing the number of false-positive alarms. An essential requirement of the sensor is that it must be extremely robust to the EM stress (R4), i.e. must not fail to alarm as a result of the stress as this is likely compromise subsequent detection. The other requirements which the sensor in particular should feature are listed as (R2 and R3).

4.3.1.2 The Detection Engine

As with conventional IDS correctly assigning the threshold for detection is the key to achieving a low false alarm rate. The function of the threshold detector [(2)] is to set a

threshold for detection above which the EM stress is of sufficient magnitude to disrupt system function. The selection of the threshold is critical to reduce false-positives and false–negatives. The usefulness of the detailed susceptibility analysis [3] is now evident as this can be used to inform the detection threshold level.

The function of elements [5] and [6] is to further reduce the number of false alarms, requirement (R10). Within the normal operating environment there may well be benign radiated and conducted transients occurring most of the time due to switch contact bounce, industrial machinery operation or mains spikes and surges for example. The function of these elements is to detect these normal unintentional *behaviours* and thereby discount them from the threat space (malicious *behaviours*).

The function of elements [7] and [8] is also to reduce the number of false alarms, requirement (R10). User confidence in the EMDDS will be severely compromised if the EMDDS indicates that a disruptive event is taking or has taken place and there is no corroborating evidence of disruption to the information process. On the other hand detection before the onset of EM disruption must be desirable. Correlating the EMDDS output with other IDS sensor outputs will therefore be useful for improving confidence to INFOSEC professionals that abnormal behaviour is taking place.

The function of elements [9] is simply to interpret the output of the detection engine as an alarm. In the simplest physical sense this could be an audible sound or visual alarm. For Cyber IDS 'pop-up' alert messages are often displayed on the computer monitor.

4.3.1.3 The Command Console

The command console for cyber IDS is generally a computer system. The IDS can be resident in the background on a users computer which therefore acts as the command console or it can be hosted on a computer dedicated to INFOSEC processes. For the EMDDS the command console could feasibly be any data logging device with sufficient processing capability together with the ability to interface with conventional IDS, requirement (R11).

4.3.1.4 Minimum Essential EMDDS

In order to provide a condensed and tractable solution the first prototype will comprise of a minimum set of functional requirements principally elements [1], [2] and [9] only. This will fulfil some minimum alerting function. The conducted threat element will not be

considered in the initial prototype development because the additional effort required is considerable and there is much less information available to accurately set a detection level. The minimum essential EMDDS to be taken forward for prototype development is shown in Figure 59.

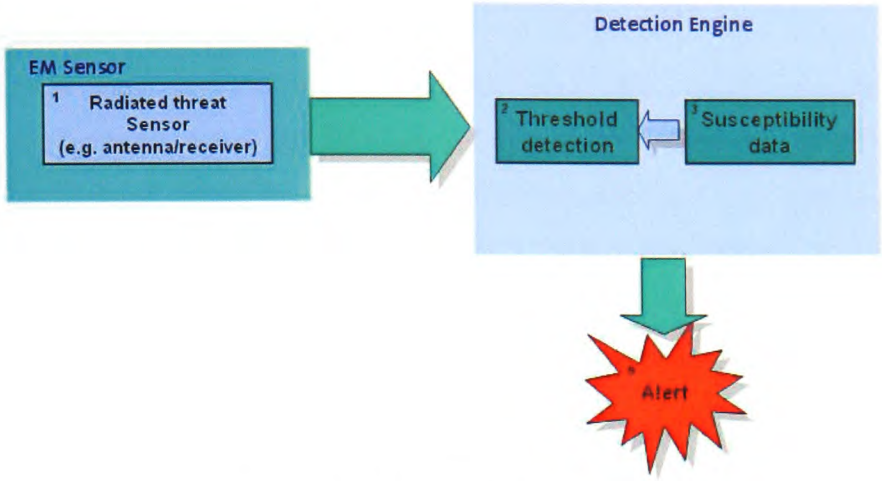


Figure 59: Minimum essential EMDDS

4.3.2 EM Sensor Candidate Technologies

The EM sensor element must act as a transducer such that the electric field stress is converted to some other parameter (e.g. voltage or current) for comparison with threshold data. It is an essential requirement for the sensor to have a very wide frequency response (R2), and a desirable requirement that it is omni-directional (R5).

From reviewing published literature on detection of highly stressing electromagnetic fields several options are initially considered and subsequently discussed in greater detail with a view to down selection of candidate technologies. These options include:

- Conventional RF receivers
- Electromagnetic Field (EMF) detectors
- Diode detectors
- Electro-optic detectors
- RF Transducers

4.3.2.1 Conventional RF Receivers

This category covers most conventional types of radio frequency receiver primarily consisting of an antenna and a broad band receiver made from electronic components. The antenna essentially acts as the sensing element with the receiver performing the transducer and detection function.

There are very many types of RF receivers commercially available which vary from handheld scanners to full-scale Electronic Surveillance Measures (ESM) receivers. However, an essential requirement of the EMDDS is that it has a very wide instantaneous bandwidth to cope with impulsive signals (R2). Most RF receivers are narrowband receivers and step or sweep through a broad frequency range. This renders them unsuitable for this application. An instantaneous bandwidth of at least 500 MHz is necessary to capture an UWB waveform. Examples of very wide instantaneous bandwidth receivers are those used for TEMPEST, EW, and UWB communications applications [DSI 1550A, 2006], [Collins, 1981], [Reed, 2005]. Generally these systems are very expensive (tens of thousands of pounds) and can therefore be discounted because of essential requirement (R9). TEMPEST receivers are export controlled so that only authorised users such as national security agencies can obtain them.

Another limiting factor for this technology is the bandwidth and the transient response of the antenna. In general very wide band antennas have a linear frequency response over one decade of frequency. Requirement (R2) requires two decades of frequency response. Whilst it would be possible to employ several antennas covering the required frequency range this complicates the design and goes against the requirement for a compact system (R8). However, there is one specialist antenna system known to have a linear frequency response over the required range this is known as a D-Dot sensor [IEC 61000-4-33, 2005].

D-Dot sensors actually measure electric displacement which is related to electric field by Equation 8.

$$V_0 = R * A_{eq} \frac{dD}{dt} \quad \text{.....(Eq. 8)}$$

Where V_o is the output voltage from the sensor

R is the sensor characteristic load impedance

A_{eq} is the sensor equivalent area (m^2)

and dD/dt is the time rate of change of the magnitude of the displacement vector D which is related to the electric field by Equation 9:

$$E = D/\varepsilon_0 \quad \text{.....(Eq. 9)}$$

Where ε_0 is the permittivity of free space

A schematic diagram of a D-Dot sensor is shown in Figure 60.

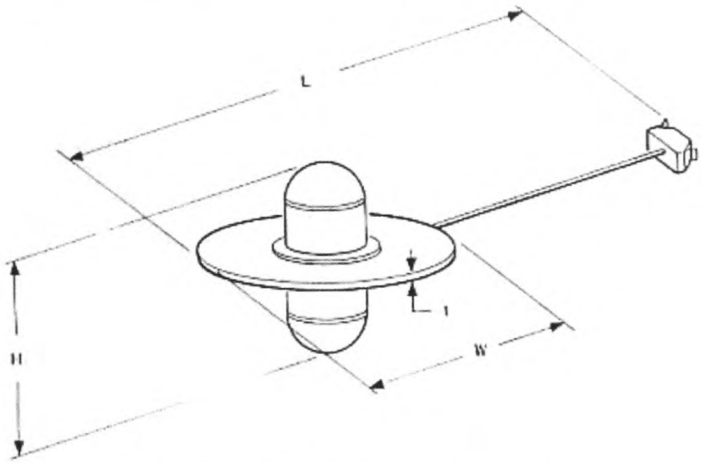


Figure 60: Schematic of the D-Dot sensor

Employing an electronic RF receiver, together with a D-Dot as the sensor element for an EMDDS has the following advantages:

- Available technology, proven for RF reception
- Ease of integration with computer network equipment (in some cases)
- Possibility of waveform characterisation (R7) although this would require development

However, there are also several disadvantages to employing an EM sensor based on this technology:

- EM disruptors are designed to attack electronic circuits RF receivers are known to be particularly prone to damage [Jonsson, 2004]
- A receiver is very difficult to protect given the scope and variety of EM disruptor waveforms [Radasky, 2006], [Delsing, 2006]. Whilst it is not an essential

requirement that the receiver should not be damaged after exposure to disruption the sensor should at the very least provide indication that damage has occurred (R4). This function does not appear to be available for proprietary systems.

- The monetary cost of a typical RF receiver is very likely to exceed that of requirement (R9).

- A family or suite of receivers/antennas would be required since the threat waveforms cover an extremely wide bandwidth. This leads to increased complexity, cost and overall an increase in physical dimensions of the EMDDS.

4.3.2.2 Electromagnetic Field (EMF) detectors

EMF detectors are commercially available for the purpose of detecting and monitoring EM environments which are hazardous for human health. International limits for the exposure of humans from non-ionising radiation [ICNIRP, 1998] (EMF's) exist to protect those working in risk areas and the general public. To this end several manufacturers have produced EMF detectors for personal dosimetry or for area monitoring [Holaday, 2006], [Narda, 2006].

EMF detectors generally comprise of a diode detector coupled together with a thermocouple based sensor which detects the energy deposited in the sensor. This is because the human exposure limits are related to the magnitude of the RF energy deposited in the human body.

Employing an EMF detector as the sensor element for an EMDDS has the following advantages:

- Available technology, proven for EMF detection

- Ease of integration with computer network equipment (in some case)

- Personal dosimetry devices are compact and battery operated

However there are several disadvantages to employing an indicator based on this technology:

- Since exposure limits are based on body heating effects the EMF detector essentially averages exposure over a period of time (6 minutes). Impulsive signals such as those characterised by Hyperband waveforms may not exceed the human

exposure limit and therefore will be undetected even though exposure to electronics can induce disruptive effects

- It may be difficult to adjust or tailor the detection threshold for a proprietary device

- The EMF detectors available do not in general characterise the detected EM field

- The cost per unit of even a basic personal dosimeter is an appreciable portion of the budget, requirement (R9). Significant development effort may be required to adapt the technology for EM disruption detection

4.3.2.3 Diode Detectors

Diode detection is the fundamental process by which amplitude demodulation is achieved in an RF receiver and is part of the detection mechanism for EMF monitors. Diode detection exploits the process of rectification. Rectification is also a significant part of the process which induces the undesirable effects in electronics (demodulation via rectification by intentional or parasitic non linear elements).

A diode is a non linear semiconductor device which conducts current in one direction only as shown by the diode characteristic V-I curve [Horowitz and Hill, 1989], Figure 61.

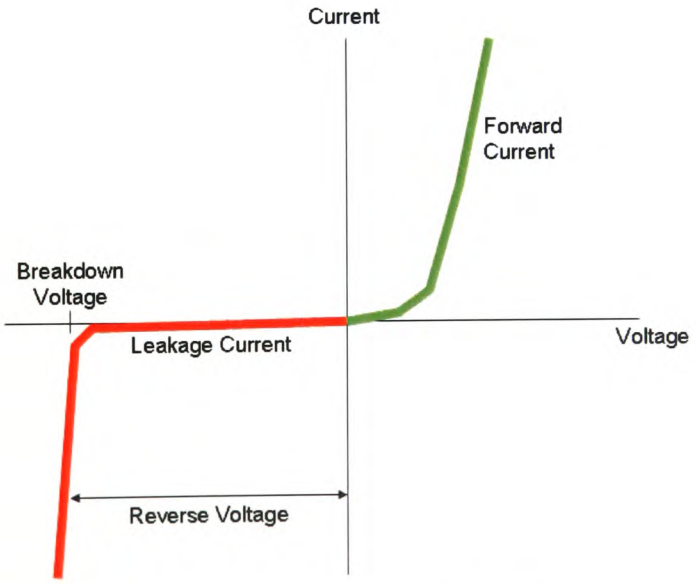


Figure 61: Typical diode V-I curve

In the forward direction (right hand side of this Figure) the diode conducts current after some minimum threshold (commonly 0.6 Volts). In the reverse direction the diode will

not conduct (although there will inevitably be some leakage current), until a breakdown voltage is reached when the diode can conduct potentially damaging currents.

A very simple diode detection circuit is shown in Figure 62.

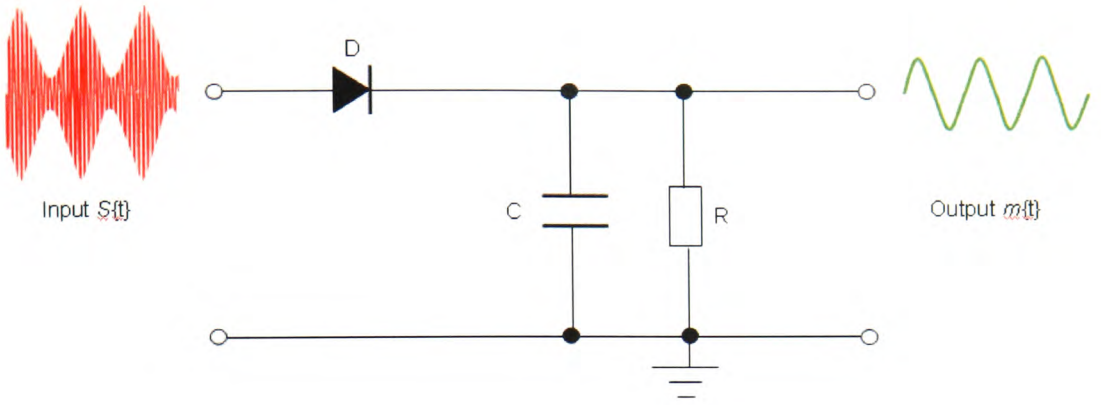


Figure 62: Diode detection process and circuit

Essentially the circuit is a half wave rectifier whereby the envelope or modulation of the input signal $S\{t\}$ is stripped off of the higher frequency 'carrier' component. The remaining output signal $m\{t\}$ is representative of the envelope of the signal and is sometimes referred to as the baseband or video signal. The amplitude of the output signal is roughly proportional to the power in the input signal.

The capacitive reactance of the diode junction but principally the capacitor C in the circuit effectively determines the upper frequency limit and therefore bandwidth of the detector. This in turn limits the minimum rise and fall time of the detector circuit and therefore the minimum duration of RF pulse that can be detected. Both the upper and lower frequency limits described in requirement (R2) may be challenging to achieve.

Examples of using this technical approach for achieving an EM field sensor/detector have been found [Dybdal, 1992], [Bassen, 1983] and to some extent are commercially available [Credence, 2005]. However, these existing examples do not meet the other essential requirements for a minimal essential EMDDS.

A bespoke design of a diode detection circuit would be necessary to achieve a workable solution. The detection circuit must comprise of a diode with a very low turn on voltage, low capacitance and high breakdown strength. The other circuit elements must also feature very low capacitance and high impedance to maximise pulse with response and

sensitivity, respectively. Some form of rudimentary ultra broad band antenna will be required to capture the RF signal.

Although this device is primarily electronic in design the simplicity and therefore low costs involved make this a viable candidate. There is no doubt that if threshold levels (i.e. the breakdown voltage) are exceeded then this device could be damaged by EM disruption. However, since the cost of a basic diode detector circuit is likely to be low (a few tens of pounds) then a simple replacement scheme could be used. Significant developmental work is required to investigate whether this simple design is effective with all types of EM disruptor waveforms.

4.3.2.4 Electro-optic detectors

The category of electro optic detectors covers any device that changes some property of light (modulation, intensity, wavelength, etc.) when an external electromagnetic field is applied. The light source is commonly a laser and the electro-optic device is usually a crystal although polar liquids are also found to exhibit the phenomenon. Electric field detectors based around bi-refringent crystals which exhibit the Pockel's effect have been found in the literature [Kanda, 1992], [Zaldivar, 2004], [Deibel, 2003] and commercial sensors are also available [Torihata, 2003].

A detector which is based on electro-optic technology such as an Integrated Optical Modulator (IOM) would comprise of the components shown in Figure 63.

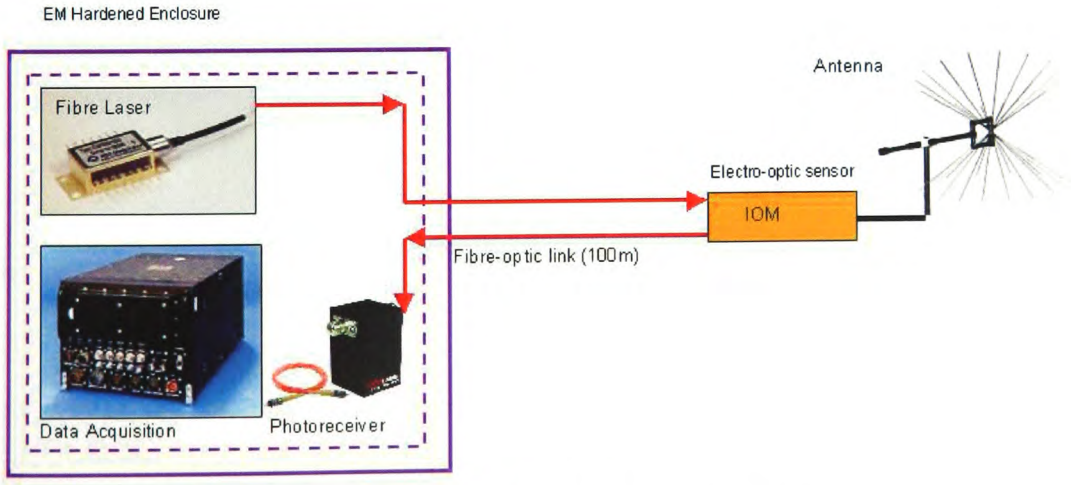


Figure 63: Electro-optic detection system components

EM Detectors based on this technology generally employ an optical fibre to connect the sensitive detection electronics to the electro-optical crystal sensor. The sensor and polarising elements form a unit the size of a matchbox which is placed in the electric

field. The laser and detection circuits may then be placed at up to 50 m away and coupled via fibre optic cable. The main application of these devices appears to be for measuring electric fields in cavities or close to structures (near field scanning) where conventional sensor types would either be too physically large or would perturb the field they are trying to measure.

Employing an electro-optic detector for an EMDDS has the following advantages:

- Available technology although not proven for this application
- Robustness, the sensing element (crystal) can withstand a large electric field without damage up to the dielectric breakdown voltage of the crystal. There is also inherent electrical isolation between the sensing element and the detection engine electronics via optical fibre
- Very wide instantaneous bandwidth of the sensing element
- Ease of integration with computer network equipment

However there are several disadvantages to employing a detector based on this technology:

- Most of the research in this area has concentrated on increasing the measurement sensitivity of the devices whereas the requirement is for a robust and fairly insensitive device. The feasibility of an indicator based on this technology is not in doubt but some development would be required to tailor the technology to this application
- The cost per unit of the necessary components is an appreciable portion of the budget. For example a high power diode laser alone can cost greater than £5,000

4.3.2.5 RF Transducers

This is a broad category covering detectors which make use of some indirect physical property to detect electric fields. Examples of this are:

1) Neon or other inert gas lamps [Thickpenny, 1971], [Yamamoto, 1995]
2) Liquid crystals [Giannini, 1977], [Sato, 1998]
3) Fuses [Seregelyi, 1999], [Eriksson, 2002]

All of these technologies are inexpensive (a few tens of pounds at most) and therefore meet essential requirement (R9). For this point alone and given the discussion above these technologies warrant some further investigation.

Neon and fluorescent lamps (both examples of gas discharge tubes) are known to fluoresce or produce a glow discharge in the presence of high electric fields. A range of conventional commercially available lamps were selected and a crude experiment was conducted to evaluate the suitability of this method of detection. The lamps were illuminated with Hyperband electromagnetic fields of varying amplitude and repetition frequency. The Hyperband waveform was selected for this test because it was suspected that the lamps would respond to energy deposition (heating) to initiate the glow discharge. Hyperband was therefore chosen because of the characteristic low average power density of this waveform type. The lamps failed to illuminate even with application of an external bias current. It is postulated that the pulse duration and average power density of the incident fields were too low to cause a glow discharge. This approach does not seem feasible at this stage.

Liquid crystal detectors have also been rejected as it was ascertained that the primary mechanism (colour change) is an average power phenomena whereby the heating caused by an incident electromagnetic field causes a change in colour of the liquid crystal material. Given the very low average power content of a Hyperband waveform there is insufficient energy deposition (heating) for this type of sensor.

Fuses are primarily used as protection devices for electronic systems exposed to over voltage or excess currents. It is postulated that the fusing (vaporisation of a thin conductor) can be initiated by high intensity electric fields as a means of detection. In a very simple design fuses are formed on thermal paper or micron thin p.c.b.'s and coupled to a planar antenna structure such as a Vivaldi antenna which provides RF signal gain. From the data available these devices appear to have insufficient sensitivity to detect Hyperband waveforms. The antenna also has to be tuned (i.e. narrowband) to optimally convert the electric field to a voltage or current stress of sufficient magnitude to vaporise the fuse. On a functional level the fuses generally require microscopic analysis after exposure to ascertain the failure method and it is known that they can be prone to damage from electro static discharge. These factors severely limit the application of fuses as transducer technologies for application to the EMDDS.

4.3.3 Summary and Down Selection

The candidate technologies are summarised in Table 30.

Technology	Advantage(s)	Disadvantage(s)	Decision
RF receiver	Available technology Waveform analysis	Likely to require a series of broad band antennas to achieve bandwidth High probability of damage Robustness Cost	Not selected
EMF detector	Available technology	Detection based on human body heating model – not suitable for detection of Hyperband waveforms	Not selected
Diode detection	Available components Low cost	Requires design/development Possibility of damage	Selected for development
Electro-optic devices	Non-electronic sensor Broadband Electromagnetic robustness	Research in this area is not directly applicable to this application Cost of components Mechanical robustness	Not selected
Neon - Glow discharge transient detector	Non-electronic sensor Compact Low cost	Requires high average power for detection - not suitable for detection of Hyperband waveforms	Not selected
Liquid crystal transient detector	Non-electronic sensor Compact Low cost	Requires high average power for detection - not suitable for detection of Hyperband waveforms	Not selected
Fuse	Non-electronic sensor Very simple Compact Low cost	Requires tuning Difficult to interrogate Not broadband so not suitable for detection of Hyperband waveforms	Not selected

Table 30: EMDDS sensor element down selection

The detection of impulses such as those produced by Hyperband EM disruptors appears to be a key limitation for many of the candidate technologies. Cost is also a significant limiting factor.

Development of an EMDDS based on diode detection was selected for further consideration. On the basis that the essential concept and principal of using diode detection for detecting EM disruptive threats to INFOSEC and given that no other

concepts of this type were found in the literature a patent application was filed for the concept at the outset of this study [Hoad, 2002].

The realisation of the concept together with potential disadvantages of this technique and especially the lack of robustness of the detector to very high power transients were subsequently evaluated.

4.3.4 Minimum Essential EMDDS Phase 1 Prototype

The diode detection principle was selected for development. An essential design driver was detection of Hyperband waveforms for the reasons discussed above. In principle the basic elements of the design incorporate the sub-systems shown in Figure 64.

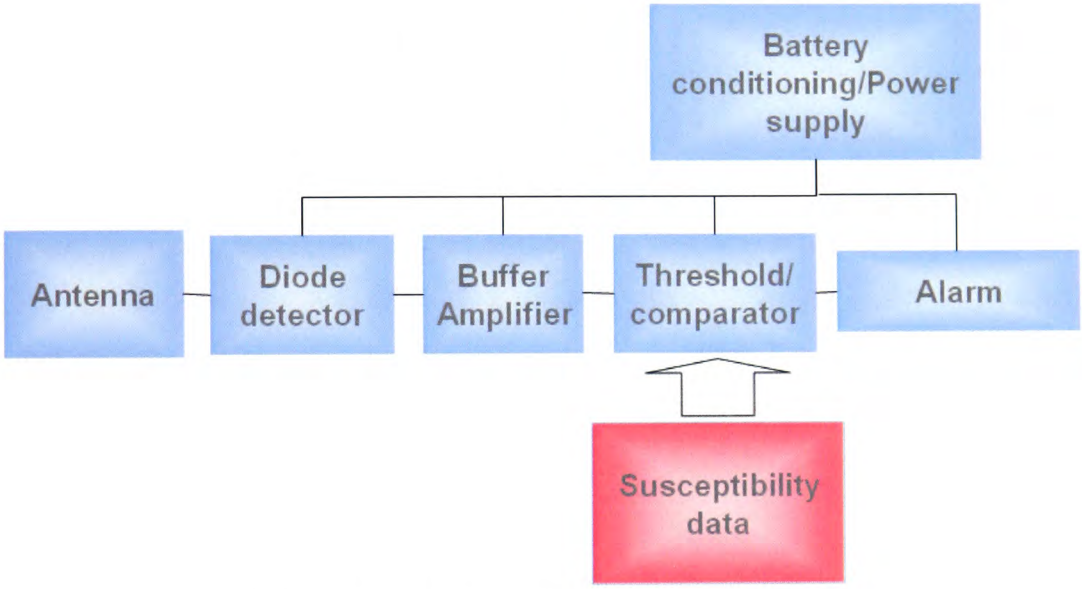


Figure 64: Block diagram of a diode based detector

Many circuit options and components are possible for each sub-system however, the essential requirement was to keep the design simple in order to keep costs manageable (R9).

4.3.4.1 Battery Conditioning / Power Supply

It is a desirable requirement (R8) that the detector should function from a battery supply. This is principally because the detector must continue to provide detection in the event of a power outage since power outage may be a consequence of EM disruptor action. Also power cables or any other conductive cables connected to the EMDDS would require careful decoupling or filtering. Cables can act as antennas coupling EM stress directly

into the system and this could skew the detector response or worse create a direct path for inducing damage to the detector.

Generally the size and longevity of the battery pack has a large influence on the packaging dimensions of the device as can be witnessed from mobile phone technology. It was therefore reasonable at this stage of the development to base the design on a single +9V supply based on a single PP3 cell.

The design also included a regulator to stabilise the battery supply output and a low power battery status monitor which provides indication of the condition of the batteries.

4.3.4.2 The Antenna

The function of the antenna is to convert the EM disruptive stress (E field / power density) into a bias voltage at the diode to enable detection. Proprietary Hyperband (UWB) antennas are not particularly compact as has been discussed. In any case the antenna should not be a separate component but ideally an integral part of the EMDDS. Perhaps the most challenging feature required is that the antenna bandwidth should ideally extend down to 100 MHz. The antenna physical length or other geometrical feature governs the resonant frequency range and therefore the effective bandwidth. A half wave dipole (a very common resonant antenna type) would need to be 1.5 m long for maximum efficiency at 100MHz. An antenna with this dimension would significantly limit the compactness (R8) of the EMDDS.

However, periodic antennas [Mayes, 1992] and in particular fractal and bent wire antennas [Werner, 2003] have been shown to offer very broadband performance in a very compact form. Fractal antennas exploit replication of geometric patterns to improve the bandwidth of the antenna.

A crude fractal or bent wire antenna design based on a square loop geometry was identified as the most practical solution. The square loop design was chosen because it was simple to implement in Veroboard (a circuit prototyping board) and p.c.b. layouts. The geometry of the antenna design is shown in Figure 65.

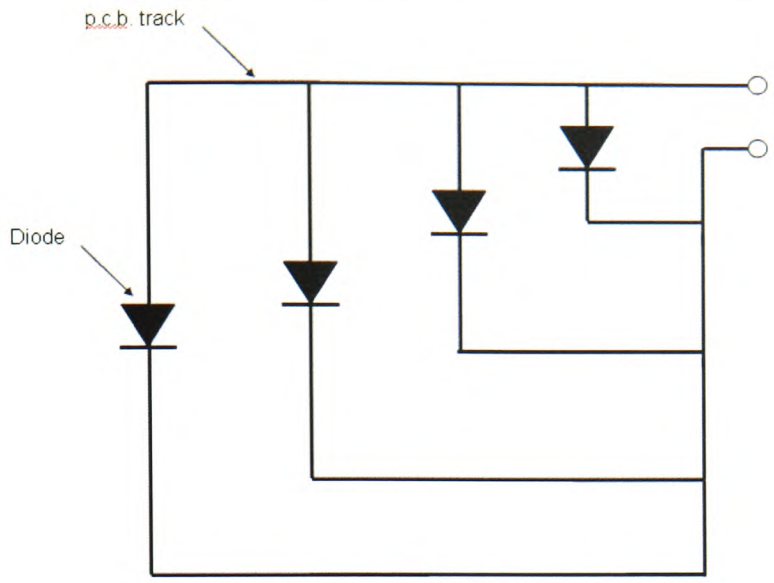


Figure 65: Nested square periodic antenna design

The overall aim of the antenna design was to utilise as many p.c.b. traces as possible to maximise the antenna wire length in a compact manner. The circuit board as a whole acts as an antenna and therefore the lengths of track between components act as resonant structures that also contribute to the length of the different antennas.

4.3.4.3 The Diode Detector

The diodes selected for the prototype was from the Agilent technologies 5082-2800 series [Agilent, 1999]. These diodes possess a very low turn on voltage (V_F) to maximise sensitivity, a very low junction capacitance to maximise the detection bandwidth and a very high reverse breakdown threshold to improve the robustness of the component. These are Schottky barrier type diodes which are the preferred types for detector applications and incorporate a 'guard ring' design implemented to increase the breakdown threshold. The 5082-2835 diode was selected for this application having the best available features these are given in Table 31.

Min Breakdown Voltage V_{BR} (V)	**Turn on Voltage V_F (V)**	**Max. Capacitance C_F (pF)**
8	0.34	1.0

Table 31: Detector diode 5082-2835 specification values

4.3.4.4 The Buffer Amplifier

In order to convert the very small diode bias voltage into a more usable voltage/current and to maximise the high frequency cut-off and impulse response of the EMDDS a buffer

amplifier circuit was used. The buffer amplifier must therefore possess a very high input impedance, very low input capacitance and very broad bandwidth. Operational Amplifiers (Op-amps) are devices which are particularly suited to these requirements. Many different types of Op-amp are available however, given that for simplicity the device should operate from a single supply rail this limits the choice of available devices.

The TLC 27 series of LinCMOS low power operational amplifiers has the following characteristics which make it desirable for this application.

Single rail operation	(V_{DD} 3 to 16 V)
Low Power dissipation	(0.05 mW)
High input impedance	(10^{12} Ω)
Good Common Mode Rejection Ratio	(84 dB Typ.)

The Op-amp was required to produce an output swing to the positive supply rail when there is sufficient rectified voltage across the detector diode. The Op-amp was configured in the simple circuit configuration as shown in Figure 66.

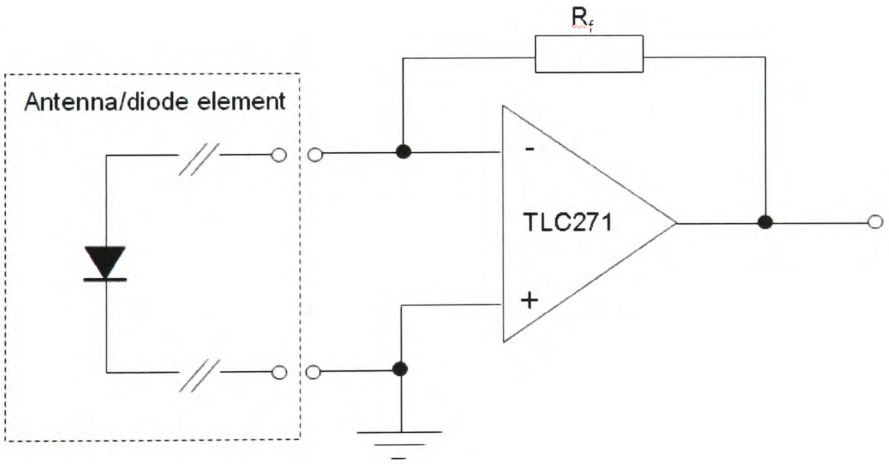


Figure 66: Buffer amplifier circuit

The feedback resistor R_f was set to a very high value so that some feedback is provided for stability of the device without compromising the very high input impedance.

The diode detector and the amplifier together formed the primary detector circuit elements.

4.3.4.5 The Threshold Comparator

The function of this circuit element is to compare the detected voltage received at the input with a pre-set reference voltage (derived from susceptibility threshold data) and to send an output signal to the alarm circuit element when the voltage from the detector exceeds the reference voltage. Many options for the threshold comparator circuit element were possible but in the interest of simplicity a 555 timer integrated circuit device was chosen.

The threshold comparator design is shown in Figure 67 and comprises a 555 timer integrated circuit configured in monostable mode.

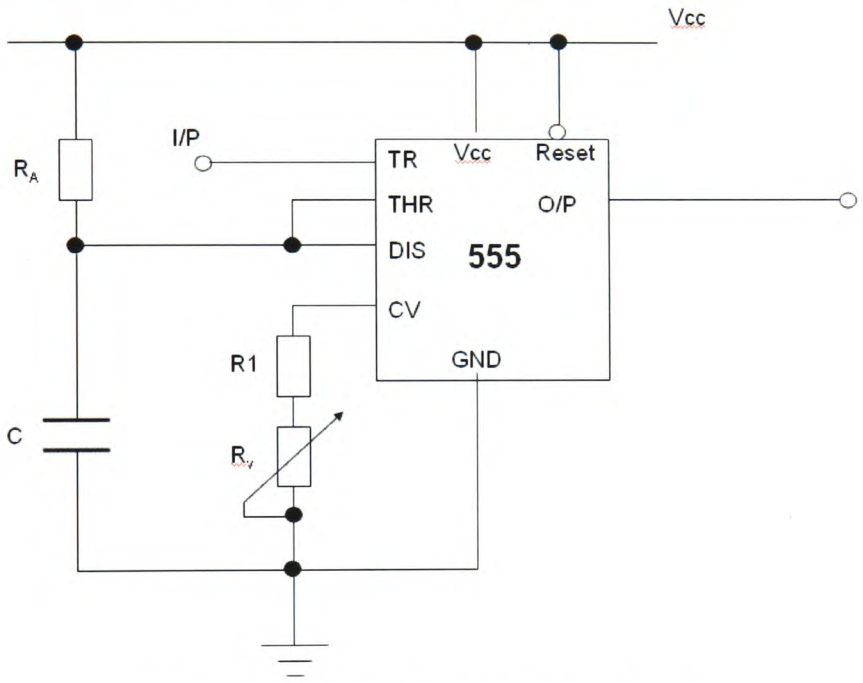


Figure 67: The threshold/comparator circuit element

The comparator circuit comprises of a variable potentiometer R_v and a fixed resistor R1 arranged in series for setting an adjustable limit for the reference voltage against which the output of the diode detector/buffer amplifier is compared. The potentiometer level is manually adjusted or calibrated to provide threshold detection at the level informed by the susceptibility test data discussed in Stage II.

The 555 timer circuit comprises a trigger pin (TR), a control voltage pin (CV) and an output pin (O/P). The TR pin acts as an input for the comparator and is connected to the output of the buffer amplifier circuit element. The CV pin is connected to R_v and R1, and the output pin is connected to the alarm circuit element. When a negative going voltage pulse is applied to the TR pin the 555 timer emits a pulse at the output pin.

The time duration of the output pulse is roughly calculated using Equation 10.

$$t_w = 1.1 R_A C \quad \text{.....(Eq. 10)}$$

Where t_w is the output pulse width

R_A is the fixed timing resistor

And C is the fixed timing capacitor

For a 40 ms pulse width (necessary for the alarm circuit element) values for R_A of 18 kΩ and a value for C of 2.2 μF were chosen. A shorter or longer output pulse can be obtained by varying these components.

The threshold comparator circuit element also comprises a latching and reset circuit. The function of the latch is to continue to provide an output signal to the alarm circuit element so that the alarm is maintained after the EM disruptive stress has subsided. This is important since it has been shown that EM disruption may comprise of a short (microsecond) burst of broadband pulses. Without a latching means an alarm generated by the EMDDS might be missed. The reset switch is also necessary to reset the output of the latch.

The latching circuit comprises of a NAND gate arranged so that once triggered the output stays at a non zero voltage.

4.3.4.6 The Alarm

As with the other circuit elements a simple, compact, and low power solution was required. It was therefore decided not to have an output which could be automatically stored or logged at this stage of the prototype development. A simplistic visual and audible alarm output was therefore chosen which was deemed adequate to facilitate testing of the prototype. A Light Emitting Diode (l.e.d.) and/a piezoelectric buzzer which are activated when an output signal from the threshold comparator/latch is received was therefore selected as the preferred solution.

4.3.4.7 Implementation

A physical prototype of the Phase 1 EMDDS implemented on Veroboard was manufactured. This prototype comprises all of those elements described as the minimum essential EMDDS and is shown in Figure 68.

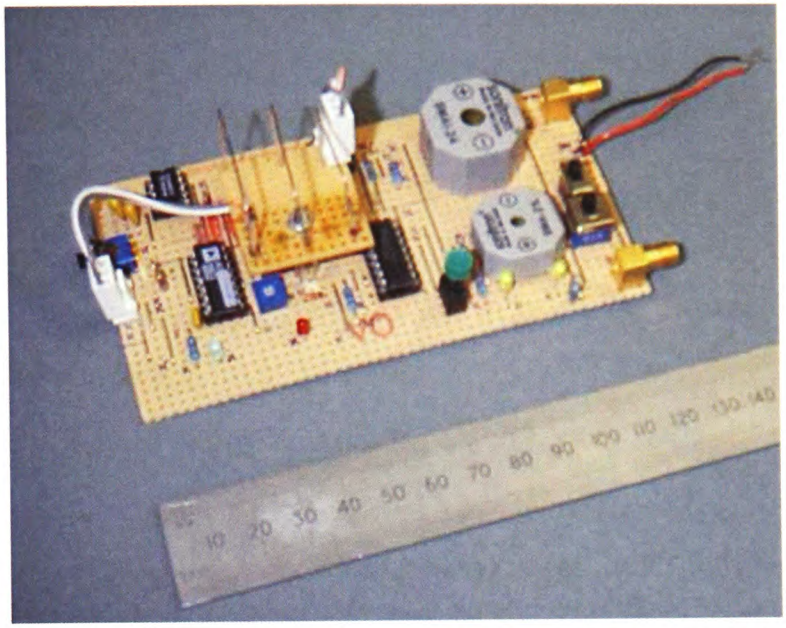


Figure 68: Phase 1 prototype minimum essential EMDDS implementation

The first prototype was implemented on Veroboard because it was cost effective, simple to modify and more convenient for diagnostic testing than p.c.b. The antenna diode element comprises of several loops implemented in vertical orientation on a daughter board above the main circuit board and connected to the main circuit board via a short cable.

4.3.5 Testing of the Phase 1 Prototype

The aims of the test campaign for the first prototype were to:

- Discover whether the EMDDS can detect the principal disruptor waveform types (microwave Hypoband, Hyperband, Mesoband and EMP)
- Find design flaws and weaknesses
- Ascertain the sensitivity/threshold of the EMDDS
- Develop a simple repeatable test protocol for evaluation of the EMDDS
- Identify improvements to the design

4.3.5.1 UWB Testing of the Phase 1 Prototype

As discussed Hyperband disruptor waveforms are considered to be the most difficult to detect because of the very high peak power, very low average power, and very wide instantaneous bandwidth. Due to the coupling efficiency factor Hyperband waveforms appear to demonstrate the lowest threshold for inducing susceptibility to computer systems compared to other waveform types. It seemed reasonable therefore to begin the test and evaluation of the EMDDS by evaluating it with a Hyperband waveform.

The data discussed previously from Nitsch et al [Nitsch, 2005] suggests that the threshold for effects to computer systems from Hyperband type waveforms can occur with a 200 Hz p.r.f. with a 2.5 ns pulse width and a peak E field of 3 kV/m. This has been equated to an effective average power density of 12 W/m^2.

It was not possible to locate a Hyperband source which provided the same pulse characteristics as the Nitsch UWB source but fortunately a laboratory UWB Avalanche pulse generator manufactured by Kentech Instruments [Kentech, 2007] became available for a short time. This pulse generator produces a bipolar Hyperband impulse with a risetime of 100 ps approx. and a Full Width Half Max (FWHM) of 250 ps approx. With this pulse generator it was possible to vary the p.r.f. from a few Hz up to 50 kHz.

The UWB pulse generator has a fixed output of 4 kV into the antenna. Calibration of the pulse generator system demonstrated that it was capable of producing up to 1.5 kV/m peak radiated E field at 1 m from the antenna. The field strength can be reduced by adding attenuation into the transmitting path.

The peak E field is lower than that of the Nitsch Hyperband pulse generator and the pulse width is markedly shorter. However, using the principle of effective average power density it is possible to calculate the range of p.r.f's available from the Kentech UWB pulse generator which are equivalent to or exceed the Nitsch Hyperband pulse generator. Given the parameters discussed, Figure 69 shows the p.r.f range where the Kentech pulse generator reaches the same effective average power density as the Nitsch Hyperband (UWB) computer susceptibility threshold.

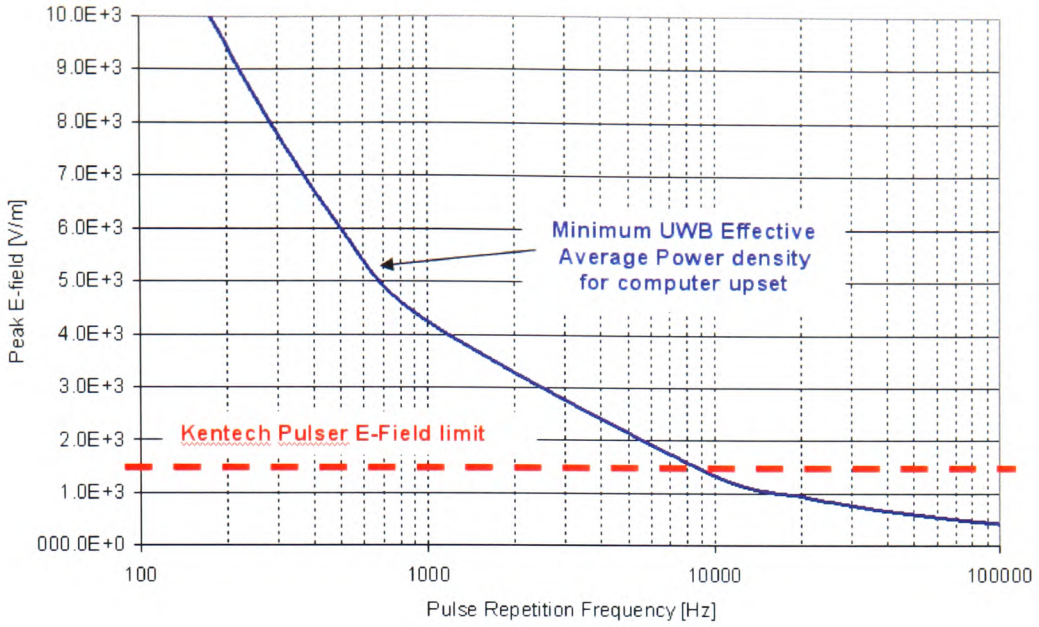


Figure 69: Minimum UWB Effective average power density curve compared with Kentech output capability

This graph shows that at the maximum output of the Kentech UWB pulse generator 1.5 kV/m the required p.r.f. must exceed 8 kHz to achieve the same effective average power density as the Nitsch Hyperband generator to achieve the susceptibility threshold.

The first prototype EMDDS was placed within the Hyperband E field generated by the Kentech UWB pulse generator. The p.r.f. was carefully controlled by triggering the UWB pulse generator from a pulse synthesiser. The test configuration is shown in Figure 70.

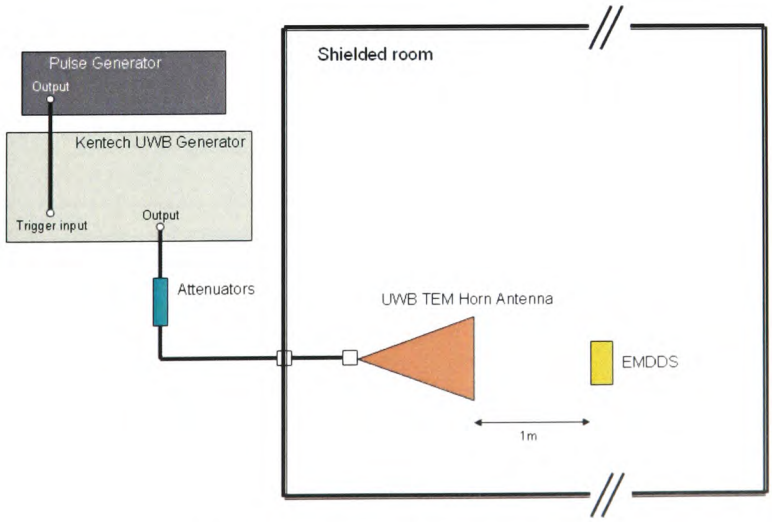


Figure 70: UWB Test Configuration

The EMDDS was placed on a polystyrene block within a shielded room at 1 m from the UWB transmitting antenna. The magnitude of the electric field was adjusted using fixed

coaxial attenuators. At fixed magnitudes (up to the maximum 1.5 kV/m) the p.r.f. of the UWB pulse generator was increased until an audible and visual alarm was produced by the EMDDS. The magnitude of the peak E field and the p.r.f at which the EMDDS produced an alarm were recorded and are given in Table 32.

Tx Attenuation (dB)	E-field magnitude at EMDDS (V/m)	Minimum p.r.f when EMDDS alarms (Hz)
0	1500	294
3	1062	328
6	752	392
8	597	454
9	532	500
10	474	541
11	423	595
12	377	662
14	299	813
16	238	1111
18	189	1515
20	150	2222
23	106	4000
26	75	7752

Table 32: Hyperband (UWB) test results for the Phase 1 prototype

The peak E field strength and p.r.f where the EMDDS produced an alarm has been plotted in Figure 71 together with the required detection threshold level derived from the Nitsch data.

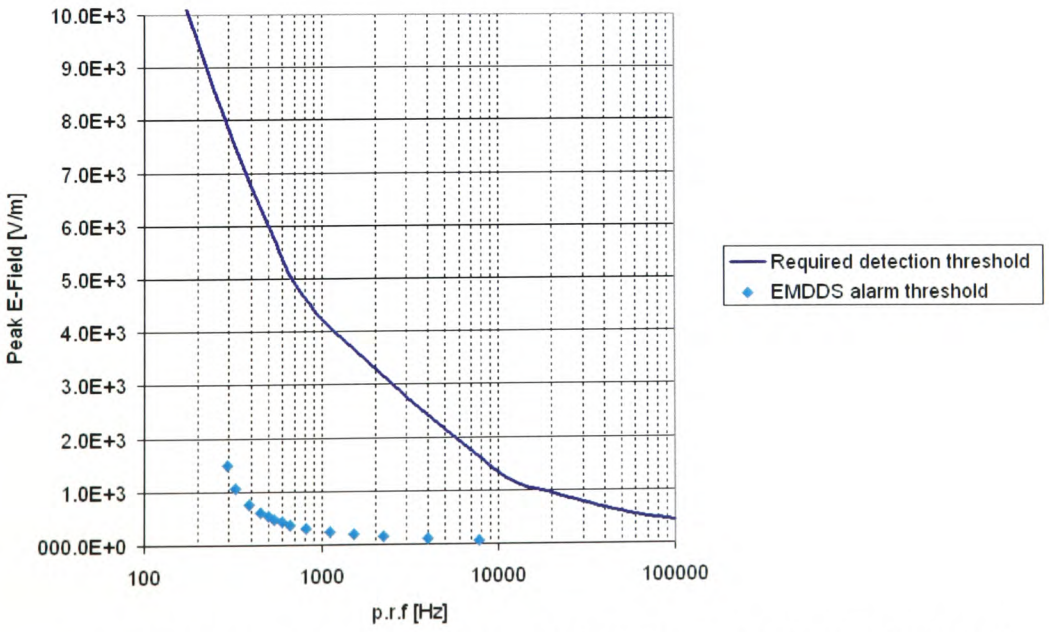


Figure 71: Phase 1 prototype EMDDS Hyperband (UWB) detection threshold in terms of peak E field

This graph shows that the Phase 1 prototype EMDDS has sufficient sensitivity to detect Hyperband disruptor waveforms. In fact the EMDDS sensitivity is below that which is required by at least an order of magnitude. The required detection threshold curve (solid dark blue line) represents the average power required to induce susceptibility to computer systems from Hyperband disruptors. Detection of disruption below this curve could lead to false alarms from the EMDDS. The threshold level potentiometer was adjusted until the detection threshold approximately coincided with a point 6dB below the required detection threshold (i.e. at half the magnitude of the required detection threshold). The figure of 6dB below the required threshold was selected as a balance between providing detection before the onset of susceptibility whilst trying to minimise false alarms. It is anticipated that if the EMDDS is deployed the threshold can be adjusted to suit the particular requirements of scenario.

The graph showing the change in sensitivity achieved through adjustment is shown in Figure 72.

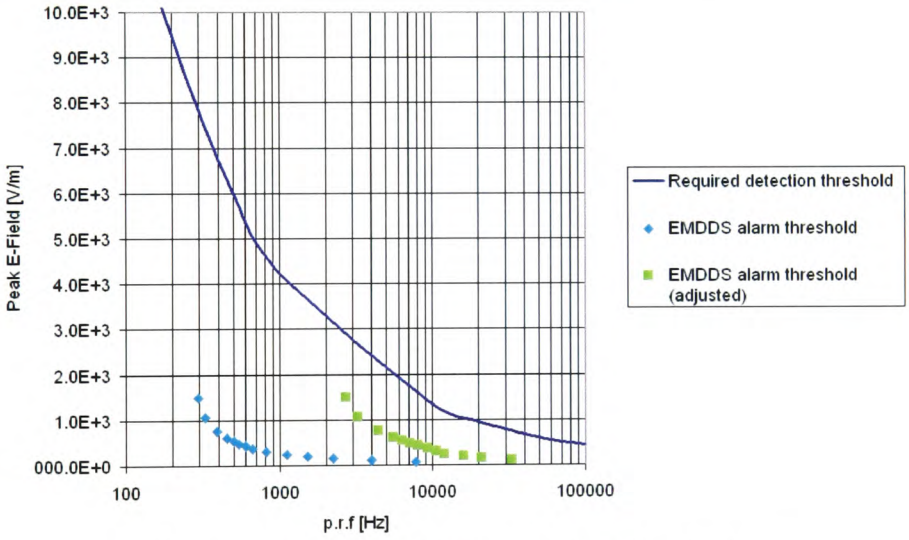


Figure 72: Phase 1 EMDDS alarm threshold adjustment

4.3.5.2 Microwave Hypoband Testing of the Phase 1 Prototype

Unfortunately it was not possible to gain access to a very high power full threat microwave Hypoband simulator such as the Orion HPM simulator at the required time largely because of the very high cost involved in conducting trials of this nature. It was therefore not possible to carry out extensive sensitivity threshold and damage testing with an HPM simulator which is representative of the state of the art.

The reverberation chamber used for the susceptibility tests discussed in Section 3.2 was also unavailable for threshold/sensitivity testing of the Phase 1 prototype. An acceptable

alternative was to make use of the QinetiQ Farnborough GTEM cell. This test facility was in lower demand because only smaller test objects (test object dimensions less than 0.5 m^3) can be tested within the cell. The GTEM cell is shown in Figure 73.

Figure 73: GTEM cell

The GTEM cell is a simple bounded wave simulator with a coaxial feed whereby RF voltage applied to the cell generates an electric field between two tapered parallel conductors (antenna elements) within the cell. The cell is loaded at the ends of the antenna elements and the sides are shielded so that there is no radiation outside of the cell. However, the GTEM cell cannot support very high power RF inputs and the capability to apply complex wave-shapes such as those typified by Hyperband EM disruptors is not possible. However it is possible to simulate Hypoband (HPM) waveforms at low power and CW input is also possible.

A 20 Watt Amplifier Research Inc. amplifier was used with the capability of generating a maximum E field strength in the test volume of 100 V/m at the 1 m separation point. A Hewlett Packard synthesiser was used to drive the input of the amplifier.

Figure 74 shows the frequency response of the EMDDS in terms of electric field strength.

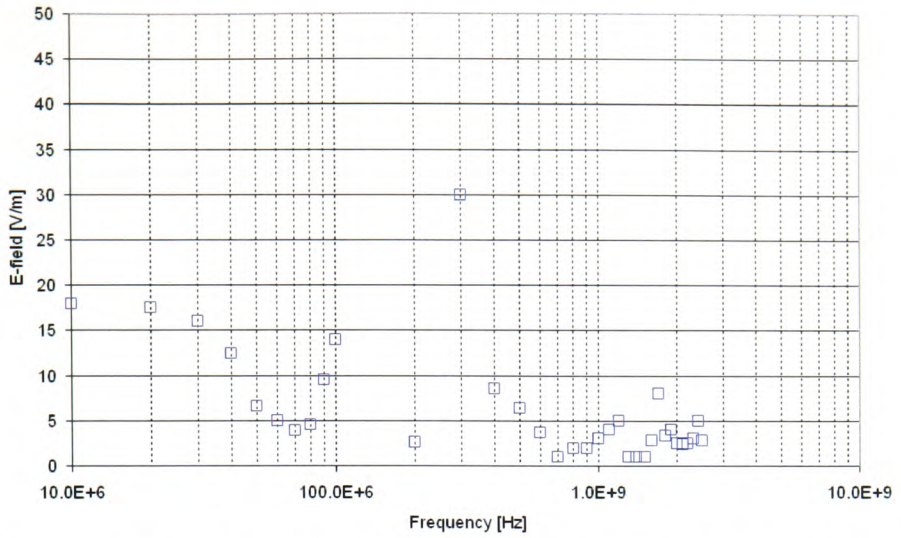


Figure 74: Frequency response/sensitivity plot of the Phase 1 prototype EMDDS to Hypoband waveforms in terms of peak E-Field

This graph demonstrates that the Phase 1 prototype was capable of detecting Hypoband waveforms across the required frequency range. However, it is necessary to define the required sensitivity of the detector for this waveform type so that the performance of the detector can be qualified.

4.3.5.3 Definition of the Required Sensitivity

The required sensitivity for the EMDDS for Hypoband waveforms required careful consideration. It was decided that a 'required sensitivity' curve should be generated from the susceptibility data for the 2.6 GHz Celeron computer shown in Figure 33 and discussed in Stage II, Section 3. This particular data set was selected from the total susceptibility data set including those data from other authors for two reasons:

1. The specification of computer (2.6 GHz) was considered to be broadly representative of the higher specification of computers found in most businesses at this time and therefore has some longevity as a benchmark

2. The data from the other authors discussed earlier has many inherent unknown factors such as, the modulation used, the EUT conditions and configuration, the accuracy of magnitude of the susceptibility threshold data and the overall uncertainty of the measurement as discussed in Section 3.6

Figure 75 shows the 2.6 GHz Celeron susceptibility data together with a curve fitted to the mean of the data set and a 'required sensitivity curve' which is 6 dB below the fitted curve.

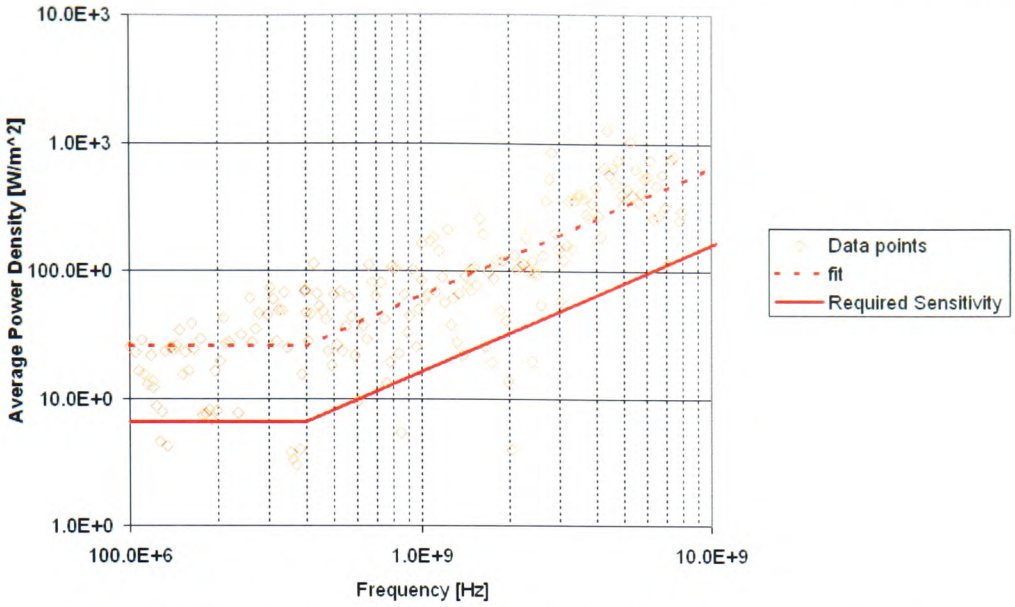


Figure 75: Fitted (red dashed line) and required sensitivity curves (solid red line)

The fitted curve is flat in the frequency range from 100 MHz to 400 MHz. This is due to the fact observed from the network test data (Section 3.5.6) that cable coupling starts to dominate the susceptibility threshold level at around these frequencies whereas aperture coupling appears to dominate at around 400MHz and above. The fitted curve from 100 MHz to 400 MHz is an average of the susceptibility values recorded in this frequency range. The fitted curve above 400 MHz is a linearly increasing 10 dB/decade change in frequency fit to the actual data. The fitted curve shape is broadly representative of the canonical coupling curve discussed in Appendix A, Section 6.5.

The actual victim system response is known to have highly resonant features. In the 100 MHz to 400 MHz region these will be due to the impinging disruptor wavelength becoming comparable with specific cable lengths on the victim system. Some of these resonant features can be seen in the graph above. However, as discussed the geometry and layout of the cable will have a large impact on the frequency at which the resonance will occur. It is therefore necessary to allow for this variance. The same variance must also be considered for the aperture coupling region. The required sensitivity curve is 6 dB below the fitted values and represents a range of likely susceptibility values which may occur whilst attempting to achieve a balance between detection before the onset of susceptibility and the creation of false alarms, as discussed earlier.

Figure 76 shows the detection threshold achieved by the Phase 1 prototype EMDDS together with the required sensitivity level.

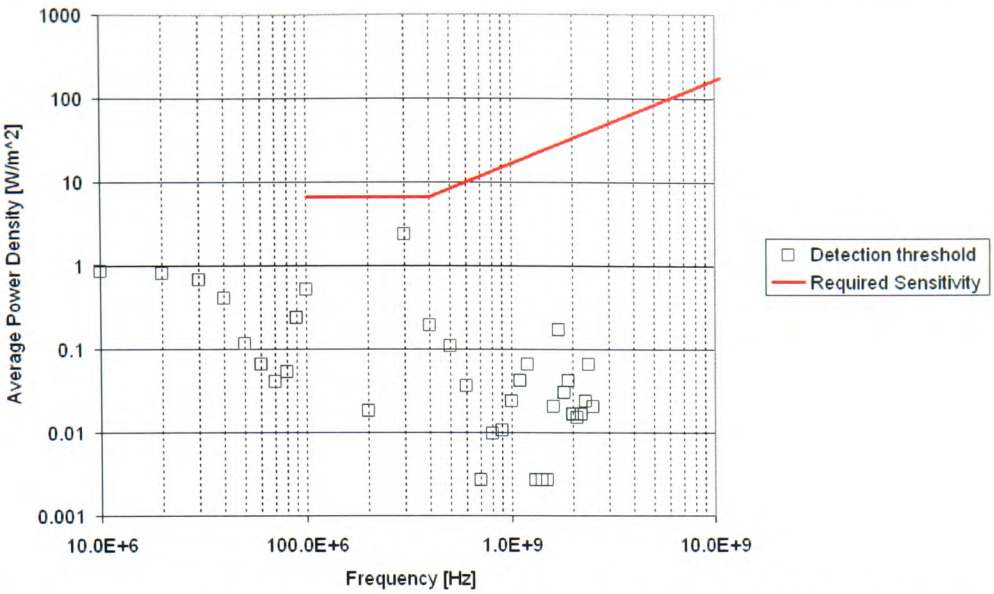


Figure 76: Frequency response/sensitivity plot of the Phase 1 prototype EMDDS compared with the 'required sensitivity' curve

It can be seen from this graph that the detection threshold of the EMDDS is below the fitted required sensitivity curve. This demonstrates that the detector is broadly capable of detecting Hypoband waveforms within the range 100 MHz to at least 2.5 GHz. Detection was actually observed up to 8 GHz but the GTEM cell is out of calibration above 2.5 GHz so calibrated values were not recorded. It should be noted that detection below 100 MHz and even down to 10 MHz was also achieved. However, detection over the 10 MHz to 100 MHz frequency range is not a requirement for the radiated EM disruption sensor. This frequency range will be addressed through the conducted detector requirement specification.

There was an apparent desensitising of the EMDDS at 300 MHz where detection was only just achieved at the maximum output of the amplifier in use (~ 20 W/m^2). It was assumed likely that this was a peculiarity of the prototype EMDDS antenna geometry. The antenna loop dimensions were modified in an attempt to shift this null point to below 100 MHz. The antenna elements required re-design in any case since a 'daughter board' and cable arrangement was more complicated and costly to achieve for a packaged detector. The Ideal design would be to incorporate the antenna on to the main p.c.b.

4.3.5.4 Hypoband Simulator Full Threat Testing

An opportunity arose to test the Phase 1 prototype EMDDS using the Orion HPM simulator located at QinetiQ Pershore. This simulator was discussed in Section 2.3.4.2.4 and produces an Hypoband waveform.

The simulator is very expensive to operate and consequently only half a day of test time was available at the end of another trial.

The Phase 1 prototype detector was placed in the Orion test range and exposed to five 200 ns pulses in a one second burst. The carrier frequency of the Hypoband waveform was 1.3 GHz and the peak E field was measured as 8 kV/m. It was found that this level was sufficient to cause damage to the detector. The failure manifested as a continuous audible and visual alarm that could not be reset.

The average power density of the burst was 170 mW/m^2 which was well within the detection range of the EMDDS, as can be seen by considering Figure 76. No damage was sustained to the detector during low power Hypoband laboratory experiments with average power density magnitudes up to 20 times greater than this level. However, the peak power density of the Orion Hypoband pulse equates to 170 kW/m^2 per pulse over 200 ns. This result indicates that the failure mechanism is likely to be related to the rate of energy deposition.

The primary detection diodes were subsequently analysed. Measurements were made of the forward resistance of the diodes which was found to be zero Ohms (specification value $\approx$ 300 Ohms). The diodes had effectively failed short circuit indicating that the high rate of energy deposition effectively caused the diode to weld across the semiconductor junction.

It was expected that the diodes would fail open circuit through vaporisation of the bond wires or the junction. This short circuit failure mode was in fact considered to be advantageous since at least an alarm was provided of the failure. An open circuit failure mode would result in the EMDDS appearing to be functional but effectively being deaf to EM disruptive threats.

Whilst the EMDDS still provides indication of EM disruption even through failure replacement of the diodes every time the EMDDS detects severe EM disruption is considered undesirable (although the actually cost of the components is only a few pounds). Given that the detector may be exposed to a wide variety of hostile disruptive environments and because of the essential requirement for the detector to be cost effective (R9) some form of diode protection is deemed necessary to improve the resilience of the EMDDS.

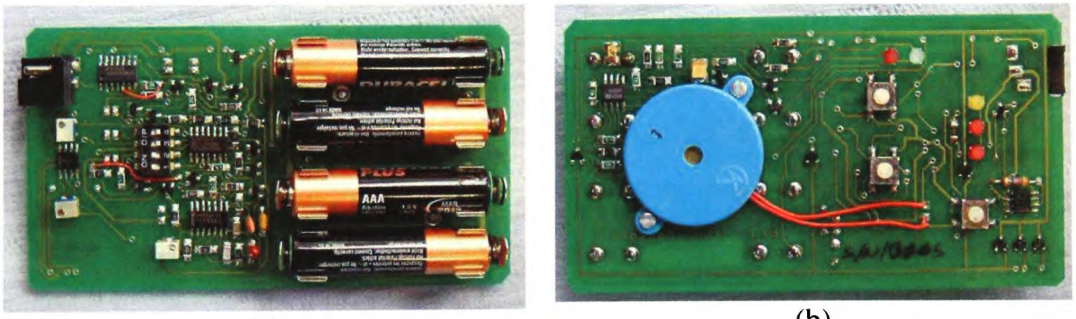
4.3.6 Phase 1 Prototype EMDDS Performance Summary

The Phase 1 prototype EMDDS meets requirements (R1), (R2) and (R3) of the minimum essential EMDDS. The prototype was demonstrated to detect Hyperband waveforms with sufficient sensitivity margin and this was considered to be a key challenge.

The Phase 1 prototype also performed satisfactorily in laboratory based experiments easily achieving the desired sensitivity level for Hypoband waveforms. However, some form of protection mechanism for the primary detection diodes was deemed necessary following full threat Hypoband simulator testing although advantageously the detector provides detection of very high power disruptive events and alarm of failure. The robustness of the Phase 1 prototype and the engineered design must be substantially improved. The EMDDS must also incorporate a data logging function to meet essential requirement (R4).

4.3.7 Minimum Essential EMDDS Second Phase

Figure 77 and Figure 78 show the re-designed minimum essential EMDDS p.c.b. and enclosure respectively.



(a) (b)

Figure 77: Phase 2 EMDDS showing the redesigned p.c.b. implementation a) topside and b) underside

Figure 78: Phase 2 EMDDS photograph of the complete assembly

The Phase 2 EMDDS featured the following improvements:

- Full p.c.b. layout
- Surface Mount Technology (SMT) design to reduce package dimensions
- Incorporation of a protection circuit and 'Hi' / 'Lo' alarms
- A single event EMP monitor
- A very low power battery status monitor circuit
- A robust enclosure
- Lower power consumption

4.3.7.1 The Protection Circuit

Following full threat HPM testing ways to improve the failure threshold were researched. This is a complex problem because many standard protection schemes (shielding, limiting etc. as discussed in Section 2.8) would affect the sensitivity or responsiveness of the detector. The chosen approach was to incorporate a more robust diode in parallel with the highly sensitive primary detection diode together with a fast semiconductor switch which removes the sensitive diode from the circuit when the more robust diode is activated. This approach is similar to circumvention techniques used for hardening and allows for two levels of alarm indication denoted 'Hi' level and 'Lo' level to be provided.

A more robust series of diodes were identified. The 5082-2800 diode was selected for this application having the best available features. These are given in Table 33.

Min Breakdown Voltage V_{BR} (V)	**Turn on Voltage V_F (V)**	**Max. Capacitance C_F (pF)**
70	0.41	2.0

Table 33: Detector diode 5082-2000 specification values

Importantly this diode has a much higher reverse break down voltage than the sensitive primary detector diode having a V_{BR} of 70V compared with a V_{BR} of 8V for the 5082-2835.

When the more sensitive diode (5082-2835) produces the detection response a 'Lo' alarm is generated, when the more robust diode (5082-2800) produces the detection response (at higher EM stress thresholds) a 'Hi' alarm is generated. Thus the alarms provide a qualitative indication of the severity of the EM stress.

Unfortunately it was not possible to get access to the ORION Hypoband simulator to evaluate the effectiveness of the protection circuit.

4.3.7.2 The Battery Status Monitor and Power Consumption

It was considered necessary to incorporate a visual battery status monitor within the detector. The function of this monitor was to alert the user that the batteries required replacement since the EMDDS would fail to alarm if the batteries were below a certain threshold. Therefore a simple blinking l.e.d. and level detection circuit was incorporated in to the second phase design.

A clear aim for this phase was reduction in power consumption. The Phase 1 prototype was found to require 80mA in quiescent (no alarm) mode. Considering a good quality 9 Volt PP3 battery with 120 mA h rating, the expected lifetime of the prototype circuit was only 2 to 3 hours. The Phase 2 design reduced the current consumption to 1mA, facilitating the use of four 1.5 V AAA cells and effectively extending the lifetime by 120 times. These cells have a very compact profile, are commonly available and can have a battery life rating of up to 1200 mA h.

4.3.7.3 EMP Monitor

An EMP monitor was incorporated in order to provide detection of single non-repetitive high peak power pulses. This detector comprises of a single 5082-2800 diode and dedicated amplifier with a latching circuit. This development was deemed necessary because the Hyperband sensitivity tests indicated that there was a limit on the minimum p.r.f. that could be detected.

A limited performance test was carried out with the EMDDS within the QinetiQ NEMP simulator. The EMP detector element was found to detect a single non-repetitive EMP pulse (t_r ~ 5 ns, FWHM ~ 150 ns) at a peak E field magnitude of 25 kV/m. The IEC EMP waveform standard has a magnitude of 50 kV/m. Therefore, this demonstrates the effectiveness of the design.

4.3.8 Performance of the Phase 2 EMDDS

The Hyperband and low power Hypoband frequency sensitivity response of the Phase 2 design was evaluated and compared to the initial prototype. The Hyperband sensitivity was found to be nominally identical to the Phase 1 prototype. The results of the Hypoband sensitivity tests are provided in Figure 79.

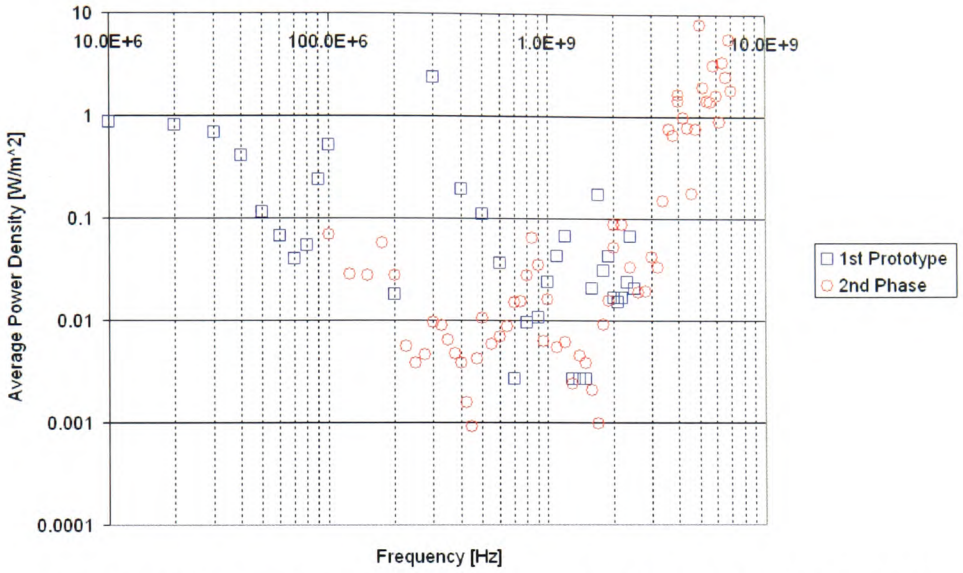


Figure 79: Sensitivity of the Phase 2 EMDDS compared with the Phase 1 prototype

4.3.9 Phase 2 EMDDS Summary

The second phase EMDDS meets the minimal essential EMDDS requirements (R1), (R2), (R3), (R4) and (R9). It is robust, portable, and proven in the laboratory experiments. The predicted build cost per unit is £1000 approx. which could be reduced significantly with volume production of the detector enclosure. This cost is well within the budgetary cost. The Phase 2 design differentiates between 'Hi', 'Lo' and EMP types of EM disruptive events.

This embodiment of the EMDDS is deployable as a standalone detector which could be positioned adjacent to potential victim computer systems to provide detection of EM disruptive threats of sufficient magnitude to disrupt computer systems. This system has the functionality to provide alarms for EM disruptive attacks which could facilitate expedient incident response and recovery.

However, the EMDDS in this embodiment does not have the utility to store data and only performs a simple alarm function. Valuable evidential information could possibly be extracted manually for example in the form of manual recording of alarm incidents by a recognised security professional.

In order to test the hypothesis of this thesis however it is necessary to expand on the minimum essential EMDDS as identified by requirements (R11) and (R13) to incorporate some form of secure data logging.

4.3.10 Minimum Essential EMDDS Third Phase

4.3.10.1 Aims for the Phase 3 Design

The primary aim of the Phase 3 implementation of the EMDDS was to provide a simple data logging feature. In the simplest form the minimum data requirement is an event time and date stamp. The type of event ('Hi', 'Lo', and EMP) would also be a useful parameter to record.

Dedicated data loggers are available but given requirement (R11) the use of a computer to act as the data logger and command console was considered to be the most suitable. The detector and computer command console can then be easily integrated with a computer network using conventional network architectures and appear like any other IDS sensor. However, one problematic issue that this concept presents is that the host computer will be susceptible to EM disruption. Specific hardening measures are therefore necessary for the computer host element of the EMDDS. This is not considered to be too onerous as many mitigation methods are well established.

A Laptop computer was used for the command console. This allows for the Phase 3 EMDDS design to be powered from the host command console thus removing the requirement for batteries since battery back up is available from the Laptop.

The Universal Serial Bus (USB) protocol [USB, 2000] allows for powering of peripheral systems components from the computer host however insufficient details of the protocol and a lack of commercially available components meant that other options must be explored. The RS 232 serial port [RS232, 2006] was selected. Whilst this port is not traditionally used to power peripherals sufficient current can be drawn from the serial port for the EMDDS application.

Finally another aim for the Phase 3 design was to completely seal the EMDDS sensor element such that there were no manual controls or indicators of any kind. Detection will be provided by the sensor as a control word using the RS232 protocol. This control word should be interpreted by the software to give status and indication information. This

design aim reduces the possibility of tampering with the hardware to affect the result which is a desirable requirement from the forensic perspective.

Obviously the Phase 3 EMDDS should have the same functionality as earlier standalone designs. A concept drawing of the Phase 3 design connected to a Laptop host/command console via the serial port is shown in Figure 80.

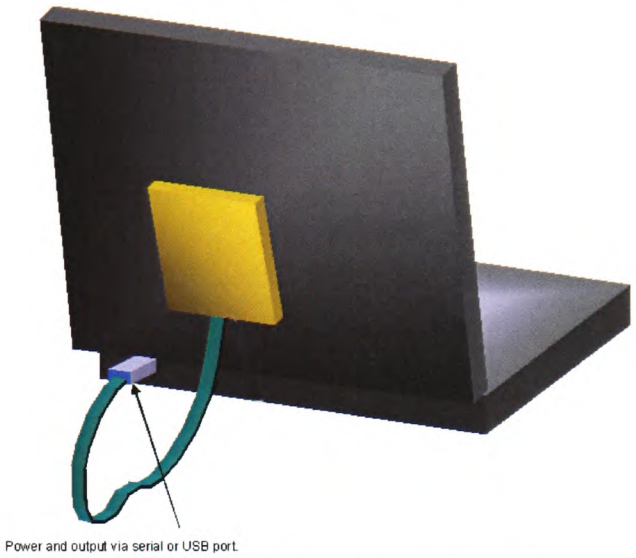


Figure 80: EMDDS Phase 3 concept drawing

4.3.10.2 Phase 3 hardware implementation

In order to assist with implementing the Phase 3 concept into a reasonable packaged design a company Laplace Instruments Ltd. were contracted to manufacture this implementation. Laplace Instruments Ltd. have a good reputation in the design and manufacture of EM test equipment including sensors [Laplace, 2007].

The Phase 3 EMDDS circuitry was implemented entirely in simple hard logic rather than more densely populated i.c. devices. A deliberate effort was made not to use micro-processors, micro-controllers or highly integrated components such as Application Specific Integrated Circuits (ASIC's) and Field Programmable Gate Arrays (FPGA's) in an attempt to avoid the problems that may occur due to the susceptibility of such devices to EM disruption.

When the EMDDS is connected to the command console it appears as a standard serial port device. Power is drawn from the Data Terminal Ready (DTR) and Request to Send (RTS) lines of the RS 232 Serial interface. The other status/control lines are monitored by the host computer to ensure that the sensor is properly connected. The EMDDS alarm data outputted on the Received Data (RxD) line and the Transmitted Data (TxD) line is

used by the host computer to check the correct operation of the sensor. Figure 81 shows a simplified block diagram of the circuitry.

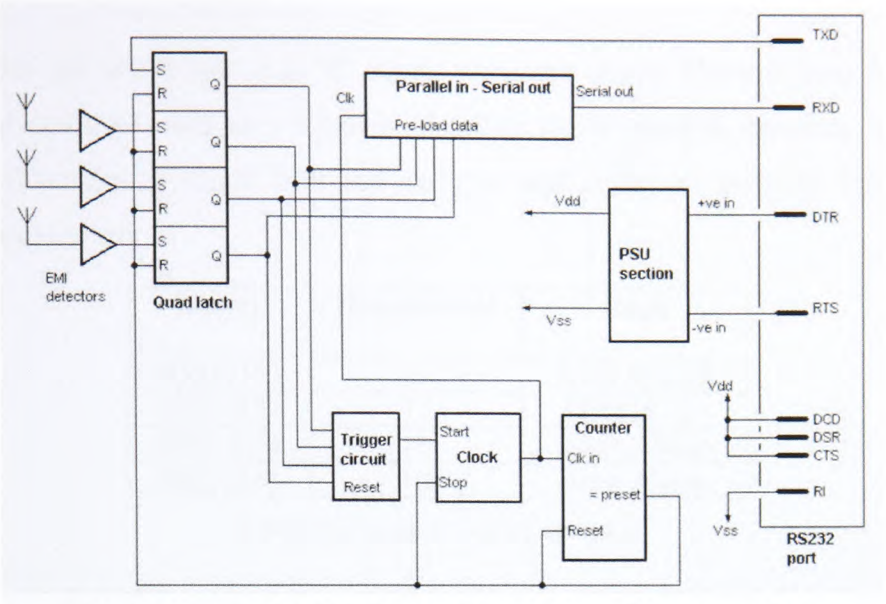


Figure 81: Simplified circuit diagram of the Phase 3 implementation

The Phase 3 design uses the standard RS 232 interface fitted to most Personnel computers. The format is 1200 baud, 8 data bits, 1 stop bit and no parity.

On an alarm event condition the sensor sends one data word (byte) containing information on the alarm event or events that triggered the transmission. There is a hold off timer incorporated within the sensor hardware which prevents the sensor from repeating a transmission for the duration of a pre-defined 100 ms timeout period. This timeout is necessary to prevent multiple system interrupts which could crash the host computer.

The byte structure of the output data word has the format shown below:

MSB								LSB
	x	x	x	D_4	D_3	D_2	D_1	1	

Where, MSB = Most Significant Bit

LSB = Least Significant Bit

x = not used – default 0

D1 = Low alarm

D2 = High alarm

D3 = EMP alarm

D4 = Serial port requested alarm status.

The data bits are active low, e.g. '0' equals an active alarm. The top three MSB's are unused and could be used as a location identifier tag if multiple detectors were to be deployed. Examples of single fault and multiple fault codes are given in Table 34 and Table 35 respectively.

Binary	Hexadecimal	Fault
0000 1111	0F	Serial Request
0001 0111	17	EM Pulse
0001 1011	1B	High Alarm
0001 1101	1D	Low Alarm

Table 34: Example Single Fault codes

Binary	Hexadecimal	Fault
0000 0111	07	Serial Request and EM Pulse
0001 0001	11	EM Pulse, High and Low Alarm.
0001 1001	19	High and Low Alarm

Table 35: Example Multi Fault codes

The alarm data word is stored on the host computer/command console hard disk in a simple text file format as shown in Figure 82.

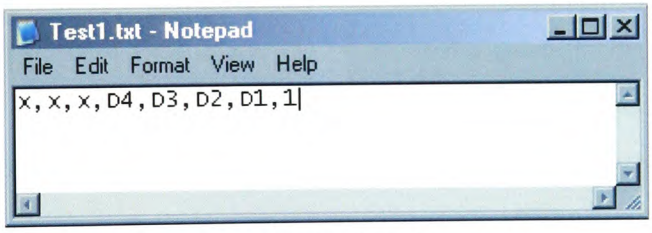


Figure 82: Simple Text file output

4.3.10.3 Hardware Protocol

The sensor draws its power from two of the RS 232 handshake lines so these lines have to be configured to the correct levels for the detector to function. The remaining handshake lines are configured so that the presence of an external peripheral device can be detected by the computer host/command console. The sensor status is reported to the host computer via the RxD line. Any character transmitted down the TxD line will trigger the EMDDS to respond with its current status.

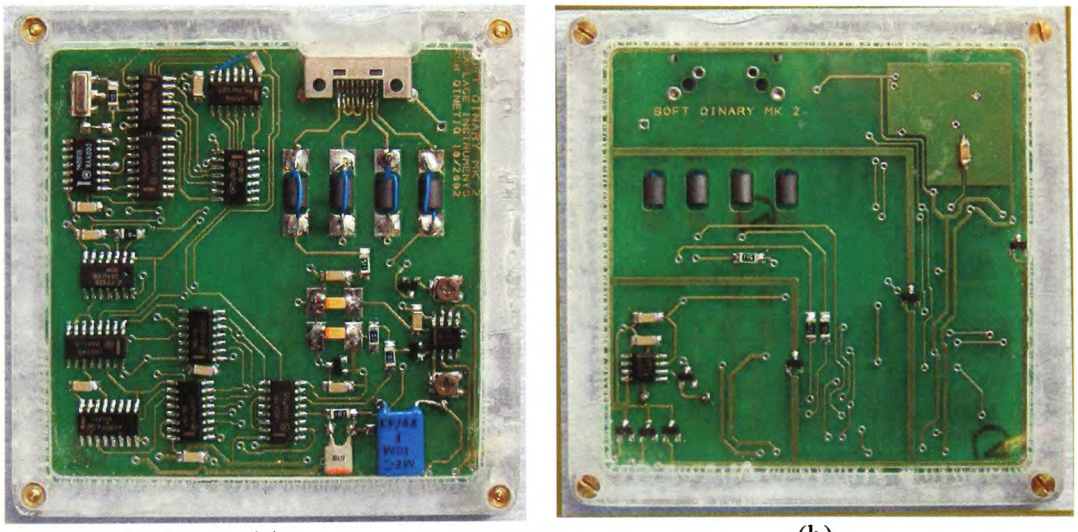
The RS 232 protocol designations for the Phase 3 EMDDS sensor are given in Table 36.

D type - 9 pin	Name	State	Function
1	DCD	HIGH	Enable EMDDS
2	RxD		Transmit data to the host computer
3	TxD		Receive status report command from host
4	DTR	HIGH	Power to the EMDDS
5	GND		Shielding
6	DSR	HIGH	Enable EMDDS
7	RTS	LOW	Power to the EMDDS
8	CTS	HIGH	Enable EMDDS
9	RI	LOW	Enable EMDDS

Table 36: RS232 Interface Port pin designation

4.3.10.4 Hardware Implementation

Figure 83 shows the Phase 3 prototype p.c.b. layout and Figure 84 shows the complete implementation connected to a host computer/command console.



(a) (b)

Figure 83: Phase 3 EMDDS showing the p.c.b. implementation a) topside and b) underside

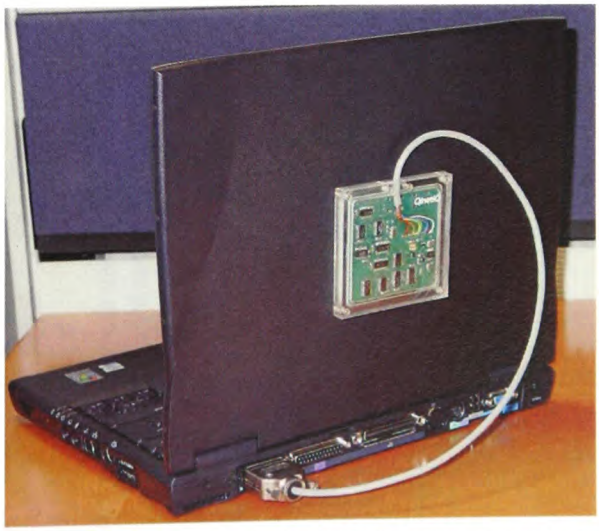


Figure 84: Phase 3 computer linked EMDDS and host computer/command console

4.3.10.5 Phase 3 Software Implementation and Functionality

A Visual Basic software application was developed to interpret the EMDDS output word and display a time stamped visual warning. This software automatically loads and becomes active every time the host computer/command console is switched on. As the software loads a message window appears briefly to remind the user that the EMDDS system has been activated. It then becomes dormant in the background although the task bar shows a small icon to show it the EMDDS is armed as shown in Figure 85.

Figure 85: EMDDS icon on taskbar

When the sensor detects a disruptive EM event a pop up message window appears mid screen on the host computer/command console. This pop up message is always 'on top' and can only be cleared by acknowledging the message. If the disruptive stress persists then the pop up indication message appears again after a 30 second interval. There are three types of message displayed in accordance with the functionality with the Phase 2 design:

- Low level EM disruption
- High level EM disruption
- EMP

These indication messages are shown in Figure 86.

Figure 86: On screen indication messages

In addition to the EM disruption indication messages two other information messages are provided:

- The software automatically checks that the sensor is connected if it is not connected a warning is given on the screen

- The software regularly checks that the sensor is operating correctly if a fault is detected a message is shown

4.3.11 Performance Testing of the Phase 3 EMDDS

The sensitivity of the Phase 3 design was evaluated in the QinetiQ Farnborough GTEM cell over the frequency range 10 MHz to 8 GHz in the same manner to the earlier Phase 1 and 2 designs. Initial tests indicated that the Serial cable acted as an antenna and the detector demonstrated abnormally high sensitivity at certain frequencies. Ferrite beads were fixed along the cable outer and on the individual wires of the cable at the p.c.b. These ferrite beads increase the loss of the cable and therefore reduce the amount of coupling. This solution solved the sensitivity problem.

Figure 87 shows the sensitivity of the Phase 3 design compared with the Phase 2 design and the target required sensitivity curve.

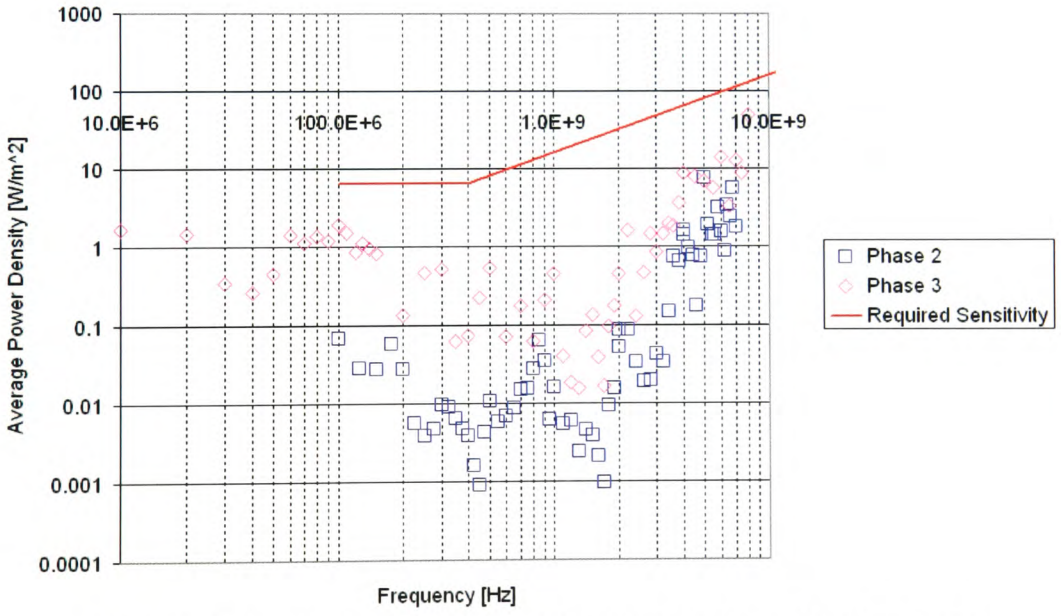


Figure 87: Sensitivity of the Phase 3 EMDDS compared with the Phase 2 prototype

It can be seen that the sensitivity of the Phase 3 design meets the sensitivity requirements for EM disruption detection. Whilst it was not possible to evaluate the performance of this design with a Hyperband waveform (a Hyperband pulse generator was not available) there is enough commonality between the primary detection circuits of the Phase 1, 2 and 3 designs to provide confidence that detection of this threat type is achievable.

The Laptop computer was also exposed during this testing and no malfunctions to the laptop occurred whilst powered via the internal battery. However, in the final implementation of the Phase 3 design it will be necessary to provide hardening measures for the laptop in the form of shielding and filtering to reduce the risk of the laptop/command console malfunctioning during an EM disruptive event.

4.3.12 Phase 3 EMDDS Summary

The Phase 3 prototype EMDDS has been developed and evaluated. This detector has all of the functionality of the standalone Phase 1 and 2 designs but has improved functionality in the form of:

- Link to computer host enabling remote interrogation
- Event log file generation
- On screen indication of disruption

The Phase 3 design meets all of the requirements of a minimum essential EMDDS, i.e. Requirements (R1), (R2), (R3), (R4), and (R9) and some of the desirable requirements (R11) and (R13). It is robust, portable, and proven in the laboratory experiments. The predicted build cost per unit is approximately £1000 (excluding the laptop/command console) which could be reduced significantly with volume production of the detector enclosure.

4.4 The Application of the EMDDS to Incident Response

4.4.1 Introduction

The primary aims for developing the EMDDS prototype are to provide detection of EM disruption and as a requirement of the hypothesis to provide diagnosis. Diagnosis of failure is useful if it can be used to respond in a timely and directed manner to malicious EM incidents and further for forensic purposes.

According to the SANS institute [Murray, 2007] there are six steps to incident Handling/Response; Prepare, identify, contain, eradicate, recover, lessons learned. The preparation step involves the setting up of an appropriate incident response policy and plan which is considered to be a vitally important stage. An expanded form of the above with respect to EM disruptive attack could be:

- Set appropriate policies – Need to understand the types of incidents that can be perpetrated using EM disruption
- Verify that an incident has occurred – EM phenomena detected as well as effects observed
- Limit the impact of the incident – Containment, isolation
- Maintain/restore/recover business continuity
- Diagnose how the attack was executed – The need for an evidence collection mechanism
- Prevent future attacks or incidents – Inform a risk assessment to identify countermeasures
- Improve security and incident response time – Lessons learned
- Prosecute illegal activity – The need for an evidence collection forensic tool
- Keep management informed of the situation and response

In order to understand the applicability of EM disruption detection to expedite incident response it is therefore necessary to understand the types of incident which could be perpetrated using EM disruption and understand forensic processes.

4.4.2 EM Disruptive Threats – Types of incident

In the context of EM disruptive threats it is perhaps important to understand the types of incident which could be perpetrated using the technology. In the context of criminal incidents then the types of crime [Home office, 2007] which could be instigated with the use of this form of technology could include:

- Criminal damage
- Arson
- Robbery of business property
- Blackmail

Of these the threat to business and business process rather than the threat to domestic situations is clearly the most interesting largely because the magnitude of the risk grows with increasing use and reliance on computer based hardware, computer based processes and electronic systems. A 2003 report by Axa business insurance services [Axa, 2003], claimed that business crime cost UK plc £8.7bn in 2002. The three most prolific crime types were criminal malicious damage, robbery and arson. All of these crime types could be committed using EM disruptors.

The business and business process in this context could refer to anything from a central government function, financial institution or manufacturing industry, through to retail industry.

In terms of High Tech crime [Kovachich and Jones, 2006] the manifestation of EM disruptor action has most in common with the end effects of DoS types of attack and perhaps logic bombs i.e. the temporary or permanent disruption of a business process or service as discussed in Stage I, Section 2.7.

Five reported [DHS, 2006], [Siniy, 2006] criminal usages of EM disruptors have been found in the literature several of these were discussed in Section 2.5:

1. In the Netherlands an individual disrupted a local financial institutions computer network because he was refused a loan – Type of crime: blackmail/criminal damage

2. In Japan two Yakuza criminals were caught using an EM disruptor on a Pachinko (gaming) machine to trigger a false win – Type of crime: robbery

3. In St. Petersburg, Russia a criminal used an EM disruptor to disable a security system on a Jewellery store, so that he could commit a robbery – Type of crime: robbery

4. In London a city financial institution was the target of blackmail attempt whereby the use of EM disruptors was threatened to be used against the financial institutions systems – Type of crime: blackmail

5. In Moscow, Russia a Telecommunications centre was targeted and was put out of commission for 24 hours denying service to 200,000 customers - Type of crime: blackmail/criminal damage

4.4.3 The Forensic Process

Forensic science can be defined as:

'...the application of science to the law... involved in the search for and examination of physical traces which might be useful for establishing or excluding an association between someone suspected of committing a crime and the scene of the crime or victim' [FSS, 2007].

And computer forensics can be defined as:

'...the preservation, identification, extraction, and interpretation of computer media for evidentiary and/or root cause analysis' [Kruse and Heiser, 2002].

A forensic investigation is primarily initiated after a crime is perceived to be committed and starts at the crime scene. The primary aim is to gather evidential information in support of a legal case against the criminal party which is prosecuted in a court of law. Each part of the forensic process must be carefully documented and this documentation forms part of the evidential information and are known as the chain of custody [Vacca, 2002].

For computer forensics the techniques can also be used to determine the root cause of an event i.e. a diagnostic process in order to identify vulnerabilities so that they can be protected from future exploitation.

The simplified process is:

1. Acquire evidence
2. Authenticate evidence – this stage has some specific attributes when applied to digital evidence
3. Analyse evidence

IDS and system log files are an important tool in the computer forensic examiners toolbox since they can identify that a malicious event has occurred and provide a log of events before and subsequent to the event.

4.4.4 The Use of EMDDS as a Forensic Tool

For computer forensics the computer can be the instrument of the crime (i.e. the hackers machine or the paedophiles storage media) or the victim (i.e. the hacked network). For the case of EM disruptors the computer or electronic process is the victim only.

In his book Kruse [Kruse and Heiser, 2002] identifies a forensic process comprised of the essential steps, Acquire, Authenticate and Analyse. For EM disruptive threats and the application of an EMDDS the techniques which could be used are discussed in the following sections.

4.4.4.1 Acquire

The process of acquisition to some extent depends on the type of crime committed however, two indicators are necessary:

1. Indication that an EM event has occurred
2. Indication that the system was in some way compromised i.e. indication that a crime has been committed

Given the discussion about the manifestation of the threat point 1 can only be provided through the use of an EMDDS. The first forensic use of EMDDS is precisely in that it aids the security professional in the detection of an EM attack. Without an EMDDS the cause of the compromise (point 2) is likely to be misdiagnosed. The second forensic use of an EMDDS then is that it aids the security professional in the diagnosis of EM attack. Misdiagnosis could potentially lead to prolonged problems this is discussed in the following section.

The EMDDS event log, time and date stamp is therefore a key piece of evidential information. Of course in order to provide a log of the event the EMDDS detector and the command console must be impervious to EM disruption hence requirement (R4). The time stamping of the EMDDS Log files of each affected system may provide evidence of the progression of the attack.

It is likely that the EM disruptor source will be mobile. Correlating the timing interval of disruption together with the physical layout of affected devices may identify the path of the mobile disruptor. For instance if several devices close to the windows on the ground

floor are affected this could indicate that the disruptor was perhaps in a vehicle moving along the street outside of the installation.

It is most likely that the indication of system compromise (point 2) will be in the form of:

- Temporary disruption of monitors, blackouts, whiteouts, flickering, banding or loss of image stability
- Temporary disruption of a single electronic device, computer reboot, 'blue screen', Latch up, loss of input functions (i.e. mouse or keyboard latch), loss of output function (i.e. no printer availability)
- Temporary disruption of multiple devices (not necessarily interconnected), denial of network services
- Persistent, repetitive temporary disruption, perhaps at random intervals
- Functional damage to devices, loss of operating environment, permanent loss of an essential input device
- Damage, permanent physical damage of components, component burn-out, may escalate to smoke and fire.

Witness statements, appropriately collected and documented should be a part of the evidential information.

Photographic evidence of the hardware device status is essential. Photographs of the visual display are important but perhaps of more value are photographs of the orientation of the affected device with respect to windows, doors, and access ways. Photographic evidence of the system cabling configuration is also very important. This evidence will provide clues to the potential location of the EM disruptor source.

The hardware device itself may provide some evidence only if there has been some physical damage. Again without the EMDDS alarm a burnt out resistor could be misdiagnosed as being caused by a routine electrical fault such as a power surge. For temporary disruption and functional damage where the software has been compromised there will be no physical evidence.

Computer log files for example the Windows Application and System event log files [Mee, 2005] may be another form of evidence. However, during the extensive

susceptibility testing of computer systems outlined in Section 3 the event log files were routinely examined and very little relevant information was found. This was discussed in Section 3.7. However, the event log files must be captured since they may help corroborate evidence from obscure data sets.

Given the indiscriminate nature of EM disruption other supporting evidence may be obtained in the form of non targeted electronics being affected i.e. the innocent bystander. Examples could include:

- CCTV camera malfunction
- Fire alarm and potentially fire suppression system activation
- Telecommunications outage
- RF receiver disruption or damage (e.g. Wifi, W-LAN)
- Electronic access failure including biometric devices
- Air conditioning malfunction (through disruption of electronic sensors)
- Nuisance Residual Current Circuit Device (RCCD) tripping and fuse failures
- Erratic traffic signalling

Again the locations of these incidents could provide clues to the location and mobility of the EM disruptive source.

Of course in order to preserve the chain of custody it is important to document every evidential item including but not limited to:

- Where was the information collected
- Who took possession
- How was it stored and protected in storage

4.4.4.2 Authenticate

The key point of the authentication process with respect to an EMDDS is making sure of the integrity of the alarm, the event log and the time-stamp.

A well established technique used for computer forensics is the 'Hash' function. A Hash function is essentially a cryptographic key calculated using a mathematical algorithm. The Hash function is generated from the parameters of the input file to be protected and is therefore absolutely unique to the file to be protected. Thus alteration of the protected file leads to the hash function being altered which provides incontrovertible evidence of tampering.

The forensic examiner therefore uses the hash function to demonstrate to a court of law that data obtained as evidence is absolutely authentic and has not been altered throughout the chain of custody.

A common Hash function algorithm is MD5 [Rivest, 1992] which outputs a 128 bit hash value sometimes referred to as a message digest as a 32 digit hexadecimal number.

There are several freeware MD5 algorithm generators available [Whitsoft, 2007], [DiamondCS, 2007] and these allow the user to assign a file to the generator for generation of the Hash number.

The EMDDS log file shown in Figure 82 which comprises of an 8-bit data byte together with a time and date stamp stored in a text file can be uploaded to the generator. A typical Hash number generated by an EMDDS log file is:

1b009a1a223bf8821cc21a3757c579e7

For the EMDDS there is no perceived need to protect the evidential detection data from tampering during or shortly after an EM disruptive event. It would require a very sophisticated attack involving EM disruption and cyber intrusion to affect the evidential data. The encryption is still useful however, because it authenticates the data showing that it has been preserved intact since detection through collection and finally through to presentation in a court of law.

4.4.4.3 Analyse

The analysis element of the forensic process for cyber crimes generally involves a very thorough piece by piece analysis of the evidence generally conducted in a laboratory environment. For example Back-ups of the drive (bit stream clone) are created and a detailed search for further evidence is undertaken.

For an EM disruptive event most of the useful evidence will be located at the crime scene as discussed in the sub-section 4.4.4.1. Analysis of the affected hardware in a laboratory may be useful if there is physical damage however, this is unlikely to help to trace the source of the attack. Evidence of damage may be useful for prosecuting some types of crime.

In all it is difficult to comment on which analysis steps will be necessary since crimes involving the use of EM disruption have not been prosecuted. Of course the credibility of the evidence and the expert witness who presents the evidence are critical as with any high tech crime.

4.4.5 Responding to an EM Disruption Incident

It has been discussed that the manifestation of EM disruptor action may in some instances appear to be similar to cyber type DoS attack. Kruse [Kruse and Heiser, 2002] proposes an incident handling process for investigating a DoS attack this flow chart is reproduced in Figure 88.

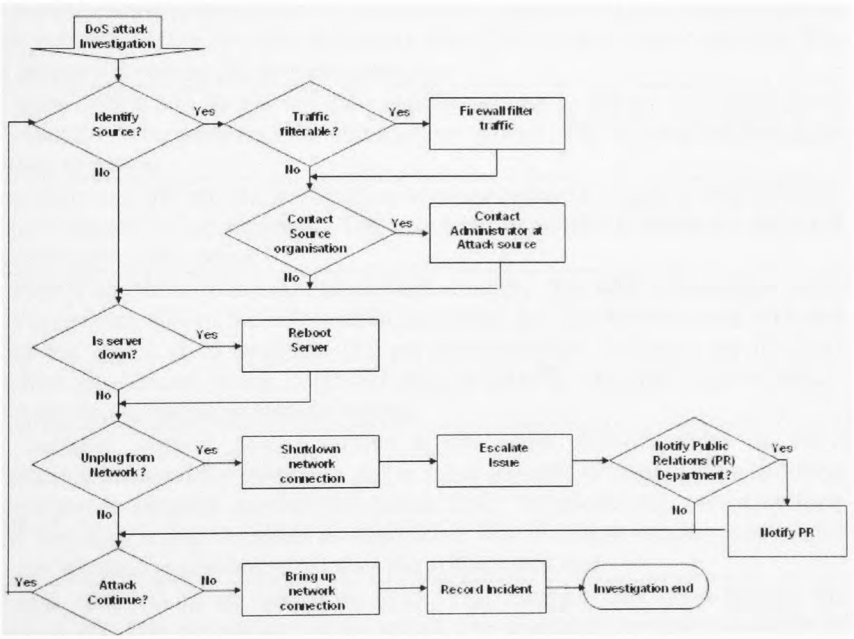


Figure 88: Process for handling a cyber DoS incident

The key point of this Figure with respect to an EM disruptive event is the first decision box. If the source of the incident is not quickly identified as being EM in origin then the disruption will be misdiagnosed and significant time, effort and resource could be expended. Consider the following fictional scenario and event history:

The victim business: A small data processing facility (32 networked terminals connected to a server, administered remotely) which could be a financial institution sorting office carrying out some time critical activity located within a larger host office type installation.

The situation: A disgruntled employee has been refused the afternoon off and decides to take matters into his own hands. He is in possession of a very rudimentary microwave oven based disruptor and decides to use it being fairly confident that it will go undetected. Rather than phone in sick or start a fire he powers up the Low Tech EM disruptor.

4.4.5.1 Condition 1 – EMDDS not deployed

Following the flowchart of Figure 88 consider the fictionalised time history of Table 37.

Event No.	Description	Time (T_0)
1.	Users start to experience strange and unexpected effects at their computer terminals. These may include monitor malfunctions, some terminals freeze, others shut down, some are unaffected. All networking operations are suspended	0 mins.
2.	The remote central administrator or Information Security Manager (ISM) is alerted to the network outage by alerts generated from IDS or other status monitors. The ISM attempts to reboot the network remotely	+5 mins.
3.	The users within the data processing facility attempt to reboot the systems that have shut down by powering the terminals on and off. The terminal malfunctions continue to persist	+15 mins.
4.	Some users call the remote information services helpdesk, multiple and different calls are logged at the helpdesk. The helpdesk dispatches a hardware technical support person to the office	+25 mins.
5.	The ISM is unable to re-instate the network remotely. The ISM immediately starts backing-up data. Given the information available, the ISM believes that a Denial of Service attack is in progress. As per the flowchart in Figure 88 the ISM examines all external facing ports and tries to identify the source of the attack. Port scans fail to reveal an external source	+ 1 hour
6.	The technical support person arrives at the scene many systems are now inoperative, permanently shutdown and it is not possible to re-boot. The technical support person suspects an electrical power fault. Telephone calls are made back to the helpdesk trying to obtain an electrician. The technical support person also asks the helpdesk supervisor to contact the utilities provider	+2 hours
7.	The data centre staff are unable to work. The manager tells them to take the afternoon off. The perpetrator of the attack (the disgruntled employee) achieves their objective	+2.5 hours
8.	An investigation is initiated by the ISM together with the utilities provider over the next couple of weeks. There is permanent physical damage to some terminals and some other electronic hardware. Some electronic hardware appears to function satisfactorily	+10 days
9.	New hardware is procured. The incident report blames power surge and power quality issues (although this is not corroborated by the utilities company)	
10.	The disgruntled employee repeats the successful attack several times, over the next few months without being caught. The loss in time, monies, and reputation of the business is considerable	

Table 37: Fictionalised incident response EMDDS not deployed

4.4.5.2 Condition 2 – EMDDS deployed

Now consider EMDDS deployment and the fictionalised time history of Table 38.

Event No.	Description	Time (T_0)
1.	Users start to experience strange and unexpected effects at their computer terminals. These may include monitor malfunctions, some terminals freeze, others shut down, some are unaffected. All networking operations are suspended	0 mins
2.	The remote central administrator or ISM is alerted to the network outage by alerts generated from IDS or other status monitors. The ISM is also alerted by an EM disruptive event alarm. A single EMDDS is located within the data centre	+5 mins
3.	The ISM telephones the office manager who in turn informs all users to stop whatever they are doing and re-locate to a nearby office	+10 mins
4.	The ISM arrives at the data centre and quickly identifies the hardware which is most affected. A physical search reveals a Low Tech microwave oven based EM disruptor located under an employees desk	+20 mins
5.	Photographic evidence is taken and the Low Tech disruptor is taken away and logged as evidence. The authenticated EMDDS event log together with other systems event logs are used to corroborate the fact that the employee was at his desk when the EM Disruptor was activated	
6.	The perpetrator (disgruntled employee) is successfully prosecuted	

Table 38: Fictionalised incident response EMDDS deployed

4.4.6 Summary

Forensics is a crucial element for gathering evidential information. Forensic evidence may be used to successfully prosecute criminal activity or to provide detailed diagnosis such that appropriate controls and countermeasures can be put in place.

Given the nature of EM disruptive events an EMDDS which can be used to produce authenticated evidence of a disruptive event will become useful for diagnosing the cause of malfunctions, for responding to incidents and for the prosecution of High Tech crimes involving EM disruption.

4.5 Stage III - Summary

Conventional 'cyber' IDS provides an essential INFOSEC function, alerting to the fact that unacceptable or undesirable behaviour is taking, or has taken, place. This alerting mechanism may deter some malicious attacks but is perhaps more useful for expediting incident response and developing and instigating mitigation and recovery strategies.

EM threats have some similar characteristics with cyber/CNA type threats and therefore concepts for the detection/indication for EM threats in a similar manner to conventional IDS have been developed.

The feasibility of providing EM disruptor threat detection has been addressed and a set of essential and desirable requirements have been produced. A technology down selection process was used and a candidate technology was selected based upon the essential requirements. An EMDDS prototype has been developed and evaluated. The prototype EMDDS meets the essential requirements and several of the desirable requirements identified.

The incident response processes, the types of EM disruptive incident and the forensic processes for gathering evidential information have been discussed. The prototype EMDDS which has been developed can be used to produce authenticated evidence of an EM disruptive event. This will become useful for attributing the cause of the malfunction to EM disruption, for responding to incidents and for the prosecution of High Tech crimes involving EM disruption. A fictionalised incident has been created to illustrate the potential effectiveness of the EMDDS for detection, diagnosis, incident response and forensics.

5 Conclusions

5.1 General Conclusions

The hypothesis tested by this study was:

'It is useful and possible to develop detection and diagnostic concepts analogous to those used to defend against conventional cyber or CNA threats for electromagnetic attacks' Section 1.1

The study has been broken down into three stages to address this hypothesis:

Stage I (Section 2) encompassed a detailed review of open literature sources and analysis of the effectiveness of EM threats from a technical capability perspective.

Stage II (Section 3) reported on extensive EM susceptibility tests carried out on computer systems and networks in order to understand information security vulnerabilities and to derive an EM disruptive threat detection threshold.

Stage III (Section 4) discussed the utility of conventional intrusion detection, demonstrated the feasibility of developing an EM Disruption Detection System (EMDDS) and reported on the potential utility of an EMDDS for incident response.

The results of the three stages above have supported the hypothesis, except perhaps that usefulness is very difficult to quantify. The usefulness (utility) of the EMDDS was discussed in Section 4.4 and in the following recommendations section.

The following sub-sections highlight specific conclusions.

5.2 Specific Conclusions

5.2.1 EM threats

It has been shown through this study that the EM (specifically the RF) spectrum can be used to exploit the confidentiality, integrity and availability of information systems. Whilst this is clearly the case EM threats are not explicitly considered in the INFOSEC guidelines largely because the risks are poorly understood.

EM *disruptive* threats which are a threat to the availability of information systems and processes were down selected from the other EM threat types (interceptors and electronic warfare) discussed for more detailed study. This was because the potential risk from EM disruptive threats to INFOSEC was qualitatively assessed as greater than for the other threat types and also to make the problem space more manageable.

It was also shown through analysis and discussion that a Low Tech perpetrator (well funded amateur) would possess the technical capability to produce an effective[9] EM disruption system.

5.2.2 EM disruptor vulnerabilities

A technically rigorous series of susceptibility experiments has shown that computer systems are susceptible to EM disruption and that the effects can manifest in a variety of complex modes. The vulnerability and impact that the induced susceptibility has on information processes is intrinsically dependent upon the information system function. Certainly, time critical processes are most at risk from EM disruption. It has been shown

[9] Analysis has also shown that the effectiveness of disruptor threats is very difficult to quantify and is dependant on many uncertain factors

that the resultant effects or manifestation of EM disruptor attacks on information systems and processes have some commonalities with 'cyber' DoS attacks.

It is postulated that in the future as society's reliance on technology grows and as technology advances (higher speed microelectronic devices operating at ever lower voltage levels) that information systems and processes and indeed society as a whole will become more vulnerable to EM disruptors. EM disruptors themselves will become more effective because of technological advances such as powerful compact prime power systems for example.

At the present time however, there is limited, clear, convincing and documented evidence of disruptor action and effects in 'real world' scenarios. It is speculated that this is likely to be in part due to the lack of understanding from INFOSEC professionals of this form of threat, the difficulty associated with human perception of this threat, and a lack of deployed detection systems.

5.2.3 EM disruption detection

Conventional 'cyber' Intrusion Detection Systems provide an essential INFOSEC function by alerting to the fact that unacceptable or undesirable behaviour is taking, or has taken place.

An EM Disruption Detection System (EMDDS) prototype based upon similar concepts of use as conventional IDS has been developed built and evaluated. The prototype EMDDS can be used to produce authenticated evidence of an EM disruptive event in order to facilitate incident response processes.

The utility of an EMDDS and indeed this thesis can be explained by referring back to the risk model shown in Figure 1 and reproduced here as Figure 89.

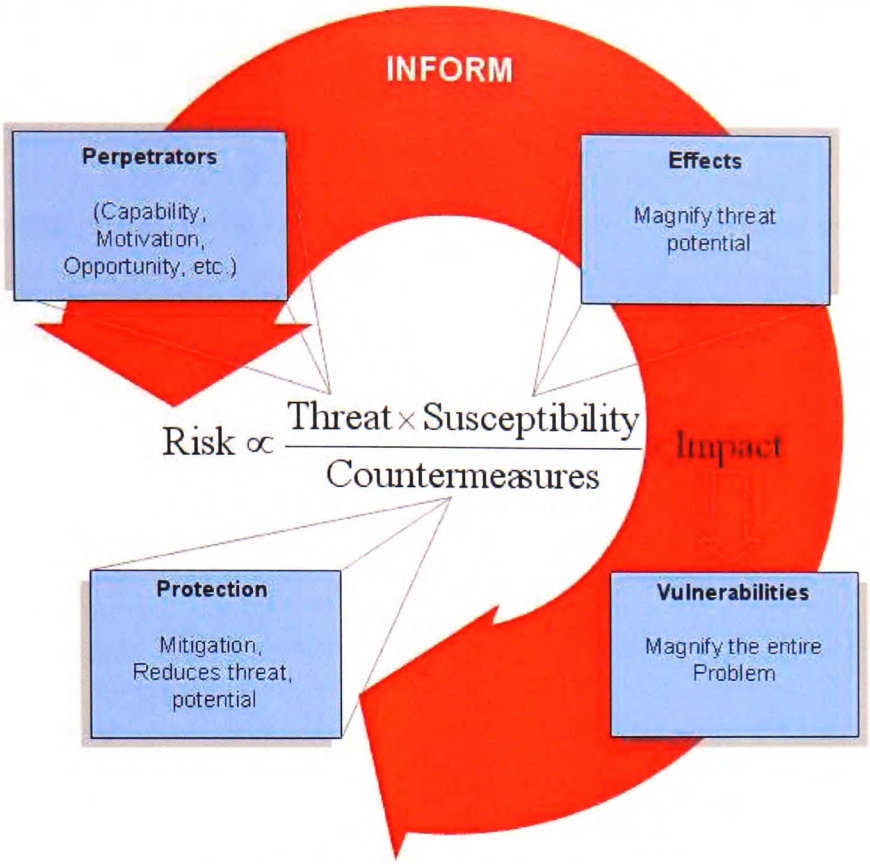


Figure 89: Risk model informed by an EMDDS

This study has shown that the threat from EM disruption is tangible (through analysis of open source references and rigorous susceptibility testing) although the impact on information processes is difficult to quantify and dependent upon the information system function. Whilst effective countermeasures (Section 2.8) for EM disruption exist it is difficult to recommend their installation as part of a balanced security approach for risk mitigation since the risk is poorly understood given current evidence.

The EMDDS system developed through this study provides detection, diagnostic and an evidence collection mechanism which will inform the risk analysis process above. An International Patent for the EMDDS has been applied for.

The EMDDS therefore allows for balanced and cost effective countermeasures to be put in place which will in turn lead to the minimisation of the potential impact of EM disruptive threats to INFOSEC.

5.3 Contribution to Science

This research has already been accepted as a contribution to the scientific community. This has principally been achieved through peer reviewed publications. A list of published peer reviewed papers is given in Section 9. Two scientific communities the

Electromagnetic Compatibility (EMC) community (Section 9, [Hoad 2, 3, 5, 6, 7, 8, 9 and 10]) and the computer security/INFOSEC community (Section 9, [Hoad 1, 4 and 11]) have published papers on this topic.

The first stage of this thesis has provided a comprehensive summary of open source discussion of EM disruptive threats. This level of detail and the subsequent analysis of the available data have not been found published elsewhere.

The second stage of this thesis has used novel experimental techniques to conduct rigorous susceptibility experiments. The results of these susceptibility experiments and the expertise gained through their conduct have assisted in the formulation of International standards for the protection of systems from high power transient phenomena through International Electrotechnical Commission (IEC) Sub Committee 77C (See Section 9, [Hoad 9]).

The third stage of this thesis details the development of a novel EM Disruption Detection System (EMDDS) for which a patent application was filed at the outset of this study. A business model for the future commercial exploitation by QinetiQ of the EMDDS for security and safety applications is under development.

5.4 Limitations

A fundamental limitation of this research has been the limited amount of susceptibility data found in the open literature. This data is essential for the accurate setting of detection thresholds. Even the experimental data produced through this research (Section 3) is sparse and insufficient to draw very clear conclusions, to estimate statistically meaningful relationships, or to develop an all encompassing theory or model. However, each item tested required the use of the reverberation chamber facility and a test engineer for approximately two weeks. The total experimental time therefore was in the order of 24 man weeks or half a man year.

The age of the technology evaluated through this study was also limited due primarily to budgetary constraints. As time progresses from publication of this thesis the relevance of the data to modern technologies is likely to be very difficult to interpret.

A fairly severe, though necessary cost limitation was placed on the EMDDS concept. Over time, EM disruptive events are likely to occur more frequently and thus the

available funding to support EMDDS development should improve allowing a variety of state of the art technical solutions to be incorporated.

It was not possible during this research to explore the real utility of EM disruption detection. It is postulated that this is best measured once the detector is deployed to support INFOSEC requirements i.e. in 'real world' operational scenarios.

5.5 Recommendations

Fundamental limitations in the availability of significant quantities of susceptibility data could be overcome by the development of an all encompassing theory or model which enables the prediction or estimation of susceptibility thresholds. However, given the nature of EM disruptive effects it is likely that this would require an extensive test and evaluation program to support and validate the theory.

At present effects data produced for government research is classified and cannot be published in the open. However, this limits the sharing of knowledge and the gearing that could be achieved from sharing data.

For the EMDDS prototype several technical improvements should be considered:

- A separate sensor for detection of conducted threats was proposed as part of the functional structure shown in Figure 58. The aim of this element will be to detect EM disruptive threats which propagate along cables these can be from a source which injects energy directly into the cable or for radiated threats (with frequency content below 100 MHz) which optimally couple to cables. As a minimum a set of essential requirements for the conducted threat sensor element should be derived ideally based on rigorous conducted susceptibility test results

- The USB standard is now well adopted and is a convenient method for powering the EMDDS. A USB version of the EMDDS should therefore be developed although some EM hardening (filtering) of the port may be necessary

- The command console used for the prototype EMDDS is a laptop computer. However, the minimum functionality required for the command console is a limited data processing capability and Ethernet compatibility. The minimum connectivity required is an Ethernet port and a USB port to power the sensor. Proprietary solutions are available that provide the minimum functionality and

connectivity required for example OpenBrick [OpenBrick, 2007]. This system is an x86 compatible single board computer with two USB ports and an Ethernet port. A compact command console of this nature could also be hardened against EM disruption by placing it within a simple shielded enclosure and filtering the power and network ports

- The other EMDDS elements shown in Figure 58 and discussed in Section 4.3.1.2 should be incorporated to limit the number of false alarms generated by the EMDDS and to assist with fine tuning of the detection threshold

- A scheme for deployment of the EMDDS should be developed. This would primarily take into account the optimum physical location of the detector within an installation. A network of deployed EMDDS sensors would perhaps provide the optimum configuration but this would need to be studied

- Ideally the EMDDS detection software should be incorporated within standard proprietary IDS software and appear like any other sensor node. This would improve INFOSEC professionals understanding of the EM disruption phenomena.

- The real utility of an EMDDS will be best assessed through deployment of the system in a 'real world' scenario over a period of time. Deployment opportunities should therefore be sought out. A business model is being developed to facilitate this

The main thrust of the EMDDS development contained within this thesis is for the application of the EMDDS to INFOSEC. However, a potential application of the EMDDS has unexpectedly arisen due to new work in the area of EMC for Functional Safety [IET Guidance, 2000]. EMC for functional safety is concerned with the growing number of safety related incidents which can occur due to unintentional or at least non-malicious EM disruption of embedded technologies. An example of this is provided below.

'Medical technicians taking a heart-attack victim to the hospital in 1992 attached her to a monitor/defibrillator. Unfortunately, the heart machine shut down every time the technicians turned on their radio transmitter to ask for advice, and as a result the woman died. Analysis showed that the monitor unit had been exposed to exceptionally high fields because the ambulance roof had been changed from metal to fibreglass and fitted with a

long-range radio antenna. The reduced shielding from the vehicle combined with the strong radiated signal proved to be too much for the equipment.' [Armstrong, 2006]

An EMDDS could have utility in several potential areas with respect to safety related functions, for example by:

1. Helping to define whether EM disruption was the stimulus which lead to a safety related incident and thereby improving with the accuracy of accident reporting statistics

2. Acting as a safety device similar in function to a limit switch or fuse for example by removing power to a potentially dangerous electronic process when EM disruption above a pre-defined threshold is detected

As an example, consider the EMC linked safety related incident discussed above. An EMDDS deployed within the ambulance vehicle could have been used to automatically switch the heart machine to a 'safe mode'. At the very least the EMDDS could have been used to indicate that and EM disruptive event was occurring thereby providing a warning to the medical technicians.

The application of the EMDDS system to safety related incidents involving EM disruption should therefore be more thoroughly explored.

5.6 Final Summary

The results of the thesis have supported the hypothesis. A thorough literature review and the subsequent analysis and experimentation have demonstrated the threat potential from EM Interceptors and EM disruptors from the perspective of technical capability. An EM disruption detector has successfully been developed and evaluated.

The usefulness or utility of EM disruption detection is very difficult to quantify although indications of utility in terms of risk assessment, incident response and forensic process have been discussed. However, the real utility of EM disruption detection may only be revealed once EM detection systems are deployed to support INFOSEC requirements. It is speculated that as technology becomes even more prolific the need for EM disruption detection and protection will emerge.

6 Appendix A – Fundamental EM concepts

The purpose of this section is to describe some essential EM concepts which are relevant to the topics discussed within this thesis. This section will consider:

- EM Hierarchy
- RF propagation loss
- Attenuation
- Antennas
- Coupling
- Signal theory

6.1 Source – Victim Hierarchy – EM interaction

In the context of this thesis it is useful to break down the typical source – victim/receptor complexity into sizes relevant to their geometry. This is useful because it is explained throughout this thesis that the geometry or dimensions of the source and victim/receptor has a large bearing on the effectiveness of EM interaction. Consider the categorisations in Figure A1.

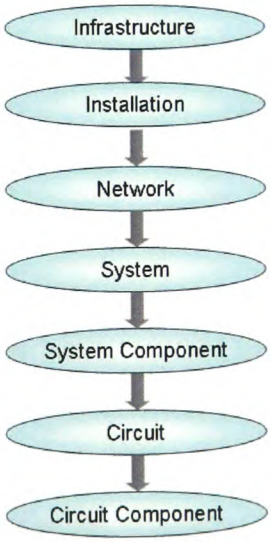


Figure A1 - Hierarchy

Infrastructure – A large National level interconnected electrical network of installations and systems, for example the National electrical power grid, Telecommunications infrastructure or a Metropolitan area Network

Installation – An office building, data centre, or other physical structure, which houses all of the elements of an information system network. The Installation may be considered as a passive element in this hierarchy in that it cannot be affected by the EM emission or interference. It can, however, modify the propagation of the EM waveform through attenuation or coupling

Network – A local area network (LAN) of interconnected information systems within an installation. This could also represent the electrical power network electrical main), or a building services network such as a fire control system within an installation

System – A collection of information system components which can be used together to deliver an information processing function such as a computer with a mouse, keyboard and power cables

System component – An individual physical element of the systems such as a keyboard or a mouse or a display

Circuit - A typical printed circuit board (p.c.b.) i.e. a Computer Mother board, a collection of circuit components

Circuit component – For example a microprocessor

This terminology has been used throughout the thesis to promote understanding of the concepts. For the purpose of this thesis the main consideration is an information system which is part of a network located within an installation.

6.2 RF Propagation Loss

6.2.1 Free Space propagation loss

The magnitude of the EM emission or RF signal propagated through the air (paths 1, 2 and 3 of Figure 3) decreases with distance from the source. In air the magnitude of the Electric Field (Symbol E, Unit Volts per metre (V/m)) will decrease at a rate proportional to the distance defined by the Equation A1 below.

$$E \propto 1/r \quad \text{.....(Eq. A1)}$$

Where, E is the Electric field strength at a distance r from the source

The normalised E-field free space propagation loss in the far field zone is shown in Figure A2.

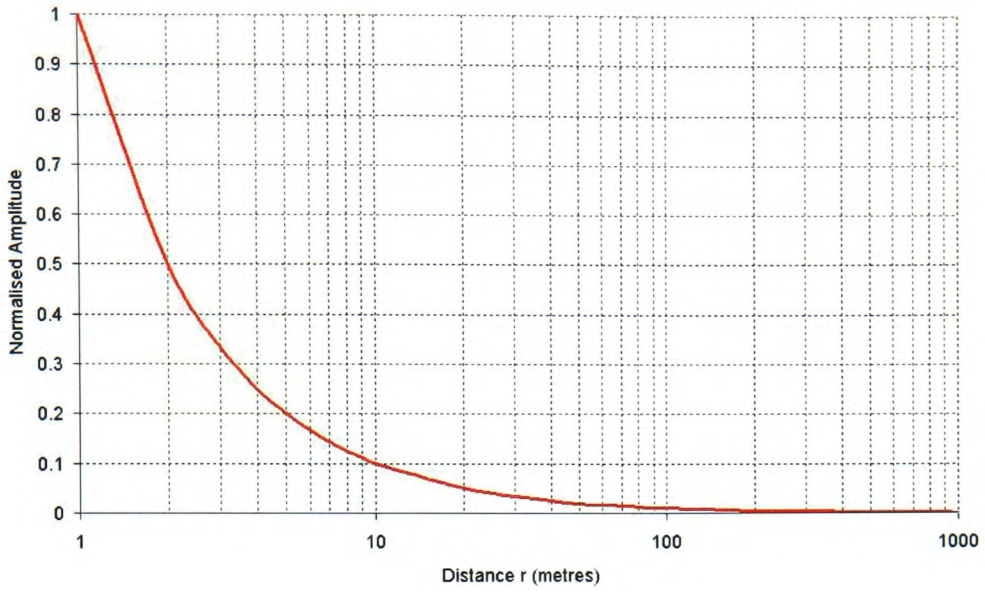


Figure A2: Graph of normalised E-field amplitude verses distance in the 'far field'

For plane waves, (a condition which is met in the far field see Section 6.2.2) the power density (Symbol S, Unit Watts per square metre (W/m^2)) and electric field strength E are related by the impedance of free space, Z_0 ($\cong 377\Omega$) via Equation A2:

$$S = E^2 / Z_0 \quad \text{.....(Eq. A2)}$$

Where, S is the power density in Watts per square metre (W/m^2)

And Z_0 is the impedance of free space equal to 120π or $\cong 377\Omega$

It can be seen from Equation A2 above that the power density falls at a rate of the inverse square compared to the electric field.

For the purpose of this thesis this means that increasing the distance between the source and the victim/receptor reduces the effectiveness of EM interaction.

6.2.2 Near field / Far field

These equations are only valid for 'far-field' conditions. The 'far-field' is a region where the electric field behaves in a predictable manner with distance from the source, i.e. the free space impedance equals 120π (377Ω) as shown in Figure A3.

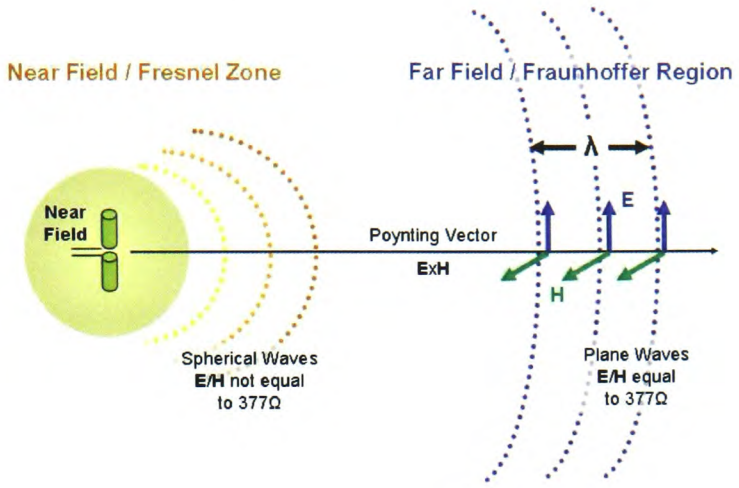


Figure A3: Near field/Far field

The zones closer to the antenna or radiating structure are known as the near field and Fresnel zones [A1: Krauss]. Within the near field the electric field strength can vary considerably and perhaps more importantly structures such as other equipment, detectors, and cables can interact and even modify the magnitude of the RF signal. The 'near field' therefore represents an unstable space.

The transition or distance from the source between the 'near field' and 'far field' boundaries is not precisely definable, but Equations A3 and A4 are used as rules of thumb [A2: Kodali]

$$Near/FarBoundary \approx r \geq \lambda/2\pi \quad \text{.....(Eq. A3)}$$

or;

$$r \approx D^2/\lambda \quad \text{.....(Eq. A4)}$$

Whichever is the greater.

Where, r is the distance from the source

D is the largest aperture dimension

And λ is the wavelength of the signal frequency in metres related to the frequency of the RF signal by Equation A5:

$$\lambda = {}^{c}/_{f} \quad \text{.....(Eq. A5)}$$

Where c $\cong 3\text{x}10^{8}$ metres per second

And f is the frequency

For the purpose of this thesis this means that:

a) Measurements of the magnitude of RF signals made in the near field are likely to have a high degree of error since the wave front is not properly formed and the measuring system may perturb the field. Extrapolation to greater ranges is therefore made very difficult.

b) Victim/receptor systems within the near field may experience different potentials across the system and may also perturb the field. Extrapolation of susceptibility threshold data for example to greater ranges is therefore made very difficult.

6.2.3 Cable Propagation Loss

The magnitude of the EM emission or RF signal propagated along a cable or along conductors (path 4 of Figure 3) also decreases with distance from the source. Again the propagation loss is proportional to the wavelength but here the situation is far more complex. This is largely because of the variety of cable types and conductor materials and the influence of the geometry or orientation of the conductor.

The typical bulk propagation loss of a normal three core mains voltage power cable found within most installations is shown in Figure A4 [A3: Eupen].

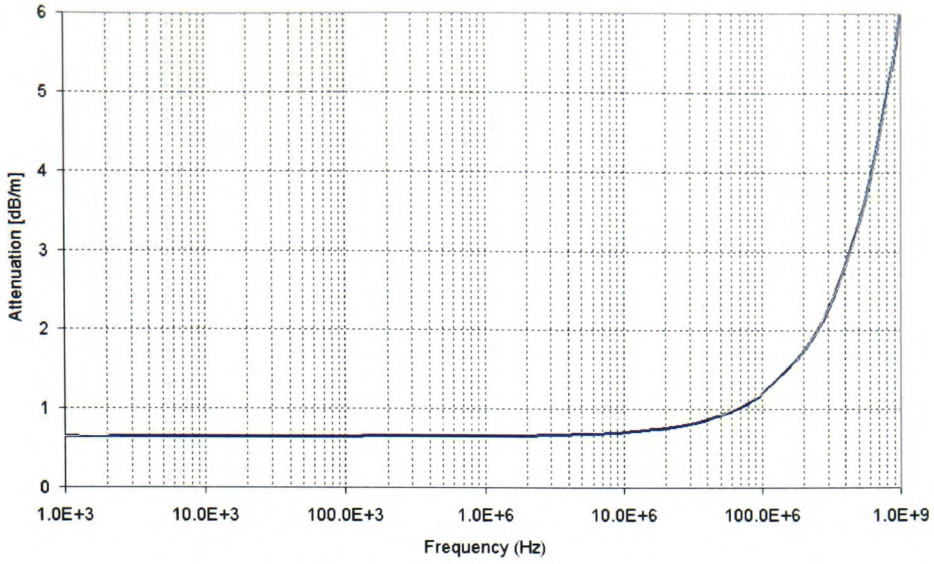


Figure A4: Power cable loss per metre verses frequency

At frequencies below 10MHz the attenuation of a typical power cable is very low, at higher frequencies the path loss increases exponentially.

A conductor such as a cable is very unlikely to have a continuous path free from junctions and connectors from outside of an installation to a given victim system. 'Lumped' components such as:

- Transformers
- Consumer units
- Distribution boards
- Fuses
- Residual current devices
- Junction bonds
- Connectors

Will attenuate (see Section 6.3) the RF signal. However, the magnitude of the attenuation is variable and complex and is difficult to ascertain although it has suggested that for typical domestic an light industrial installations the attenuation is between 2 and 40dB at 150kHz [A4: 50065].

For the purpose of this thesis this means that increasing the distance between the source and the victim reduces the effectiveness of EM interaction especially for frequencies exceeding 10MHz.

6.3 Attenuation

Attenuation can be defined as a reduction in magnitude of a signal as it passes through a transmission medium. Attenuation is usually quoted in decibels (Symbol dB). The dB is a logarithmic unit used to describe a ratio i.e. the ratio of the received magnitude divided by the applied magnitude. Attenuation is a useful concept when considering the penetration of EM energy through solid materials or structures. The mechanism of attenuation can be either reflection or absorption and will in practice consist of both factors but the magnitude of each contribution is not revealed by the concept of attenuation.

For an installation or the enclosure of a system, structures or barriers in the path of the RF emission signal such as the wall of the installation will reduce or attenuate the magnitude of the RF signal. However, not all materials have the same attenuation and the level of attenuation can vary with frequency. Some materials such as plasterboard, general partition materials, and window glass are virtually transparent to EM energy [A5: Pauli]. The graph in Figure A5 shows the attenuation provided by some common construction materials.

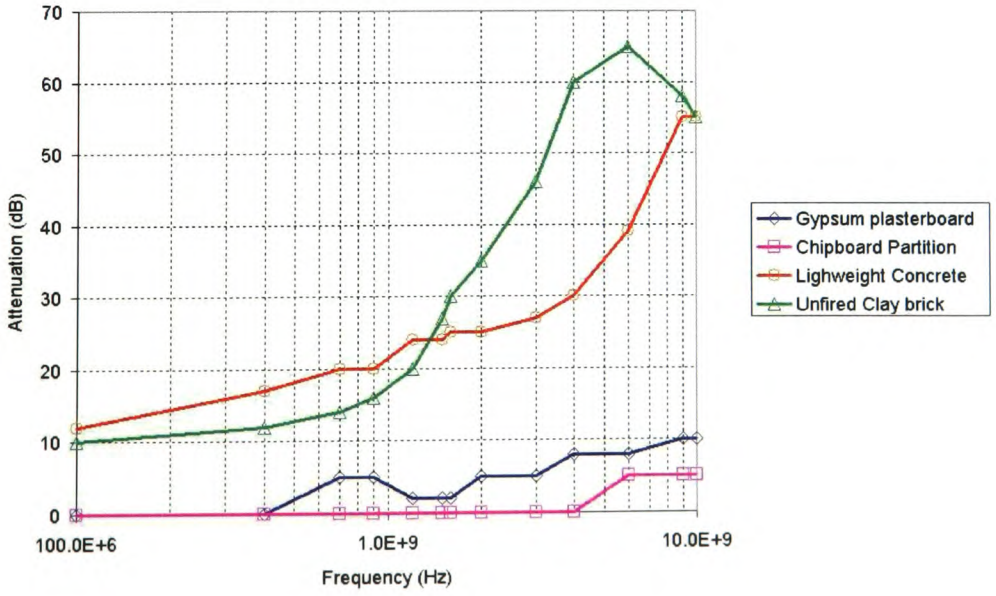


Figure A5: Attenuation of common construction materials

In this graph it is clear that materials such as brick and concrete provide superior attenuation to plasterboard and chipboard. For most frequencies the attenuation provided by the brick and concrete materials is 10 to 40 dB greater than for the other sample materials. For a barrier with an attenuation of 20dB the magnitude of the Electric field of an RF signal will be reduced a factor of 10.

It should be noted that penetrations or apertures, such as windows or doors, into a installation may offer an un-attenuated path for the signal to propagate through. However, this is again complex because the 'pass band' of an aperture will be dependent on the size of the aperture and the wavelength of the RF signal.

Apertures will pass RF energy without attenuation when the wavelength of the RF waveform is a factor smaller than the aperture dimensions. It is generally accepted that Ott's Equation (Equation A6) [A6: Ott] for aperture penetration gives an approximate measure of the attenuation provided by a regular rectangular shaped aperture (i.e. acceptable for windows and doors).

$$SE = 20\log_{10} \lambda / 2l \quad \text{.....(Eq. A6)}$$

Where SE Refers to the Shielding Effectiveness in dB

l is the longest dimension of the aperture in metres

And λ is the wavelength in free space in metres

Effectively, this equation is only relevant for an aperture in a conductive sheet such as steel, in practice materials such as concrete used for installation will cause the frequency peak to shift, however, the amount of shift is difficult to predict for a generic case. The angle of incidence of the impinging field will also skew the effective aperture size. A plot of the shielding effectiveness of a 1.5 m aperture (typical office window size) is given in Figure A6.

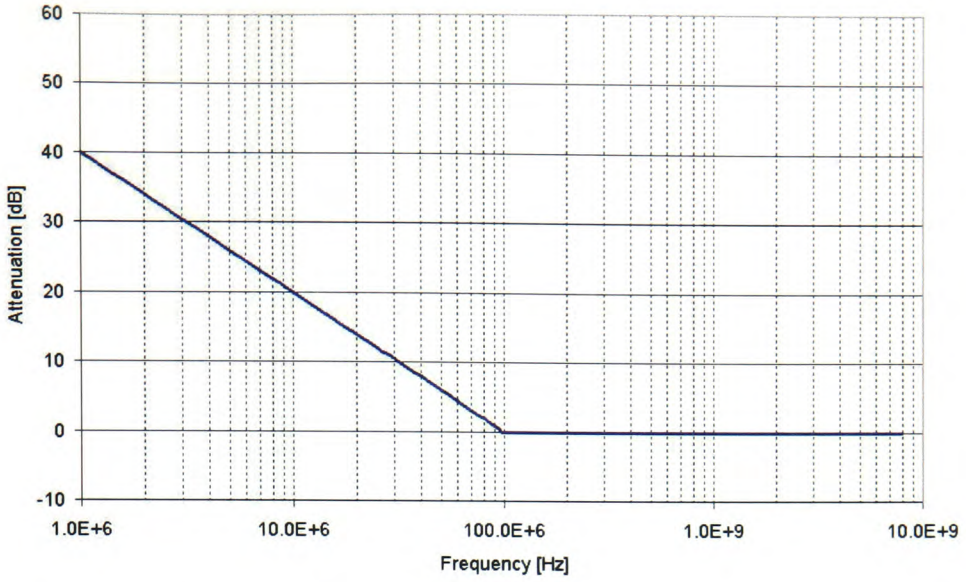


Figure A6: Application of Ott's aperture equation for a 1.5m aperture

An installation will have many apertures such as windows perhaps with complex geometries, apertures may be formed by the crossing of steel construction members and re-bar, so for a complete installation the attenuation of the structure is rather more complex. Figure A7 shows the measured attenuation [A7: Hoad] (green curve) of a three story office building compared with published data for building and construction material attenuation.

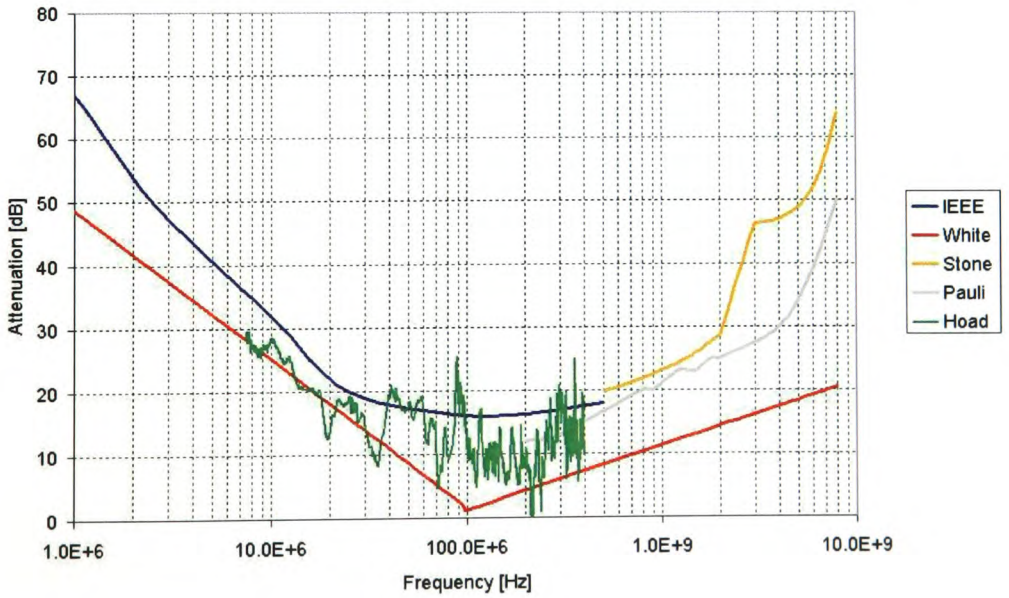


Figure A7 Measured Installation attenuation compared with published data

Note 1: The IEEE data [A8: IEEE] is based on a sample of three multi-storey office buildings

Note 2: The Stone data [A9: Stone] represents bulk attenuation of a concrete sample slab thickness = 305 mm

Note 3: The Pauli data [A5: Pauli] represents bulk attenuation of a lightweight concrete sample slab thickness = 300 mm

Note 4: The White data [A10: White] is representative of a building with a steel frame construction with facades of brick, concrete, stone and glass

It can be seen that the data from White represents the most pessimistic case when compared with the other data sets. The peak at 100MHz in this data is most likely due to propagation through apertures such as windows or through constructive interference from the vertical components of the steel frame at $\lambda/2$ spacing used for construction of the installation. The White data is obviously smoothed to remove resonances in coupling due to multiple apertures. These resonances can be seen in the measured experimental data.

For the purpose of this thesis this means that the installation construction materials and composition may reduce the effectiveness of EM interaction.

6.4 Antennas

An intentional antenna is a resonant structure with a defined geometry set to efficiently radiate or receive RF power. To quote Krauss [A1: Krauss]

'an antenna is a region of transition between a radio wave guided by a transmission line and a free space wave'

Apertures and conductors can form unintentional antennas which efficiently radiate or receive RF power at there 'natural' or resonant frequency.

The simplest antenna is the half wave dipole or doublet, where the length of the antenna arms are equal to (resonant with) a half wavelength of a specific frequency. More complex antenna types are discussed throughout this thesis the main design aim of an antenna is to efficiently match the impedance of the source or the receiver to free space.

6.4.1 Antenna gain and directivity

Gain is a measure of an antennas ability to capture energy from a free space RF signal or to deliver RF energy to a particular point in free space. The gain value for an antenna is described by the ratio in Equation A7:

$$G = \frac{\text{Maximum radiation intensity of actual antenna}}{\text{Radiation intensity of a lossless isotropic antenna with the same power input}} \quad \text{.....(Eq. A7)}$$

Where, the lossless isotropic antenna is a perfect (and therefore not realisable) antenna which radiates the same power in all directions with the same efficiency. Measurement of the power density at any point on the surface of a sphere centred on the antenna would yield exactly the same result as any other point on the sphere.

Consider the normalised radiation pattern plot, Figure A8 of two fictitious antennas a) an isotropic radiator and b) an aperture antenna such as a horn antenna.

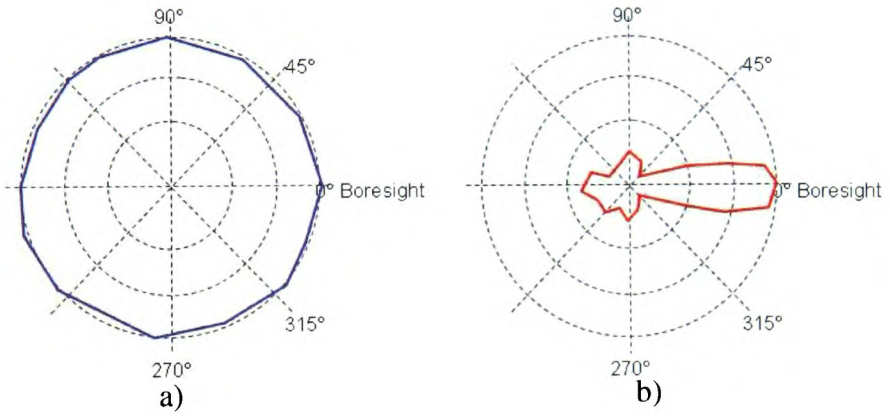


Figure A8: Normalised radiation pattern for (a) an isotropic radiator and (b) a fictitious aperture antenna

It can be seen that for the aperture antenna the power density on the surface of the sphere on boresight i.e. directly on the line of sight of the antenna aperture is much greater than for the isotropic case.

Directivity is a function related to the gain function of the antenna. The gain value takes into account the losses (thermal, reflection, etc.) of the antenna whereas the directivity function is described in Equation A8:

$$D = \frac{\text{Maximum radiation intensity}}{\text{Average radiation intensity}} \quad \text{.....(Eq. A8)}$$

The directivity is an important function of the antenna because ultimately it limits the region in space which can be effectively 'illuminated' by the antenna. Figure A9 illustrates this point.

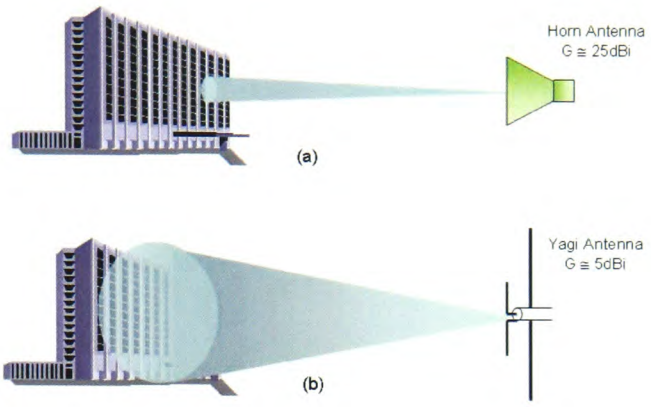


Figure A9: Implication of directivity for (a) an aperture antenna (b) a low gain antenna

Antenna gains at microwave frequencies can be of the order of 30dBi. For a radiation source this represents an increase in the power density at a point in space of 1000 times compared with an isotropic radiator.

6.4.2 Antenna Factor

The term antenna factor is often used to simplify the gain equation to a ratio of the electric field strength at a specific distance divided by the voltage supplied to a matched load, Equation A9.

$$AF = E/V \quad \text{.....(Eq. A9)}$$

Where, AF is the antenna factor in units of m^{-1}

E is the electric field at some specific distance

And V is the load voltage

A large AF is equivalent to a high gain.

For the purpose of this thesis this means that antenna gain is a useful function for EM disruptors as it potentially helps deliver more power to the victim and for EM

interceptors as it helps in converting more of the available RF power into signal. However, this is at the expense of directivity as discussed.

6.4.3 The radar equation

Equation A10, commonly termed the radar equation describes a way of deriving the power density at a point in space distance r from an antenna, with a given source power P_t and a known antenna gain G.

$$P_D = {}^{P_t G}\!/_{4\pi r^2} \quad \text{.....(Eq. A10)}$$

The denominator of this equation describes the volume of a sphere, which is a perfect loss less omni-directional (isotropic) antenna. This sphere is modified by the antenna gain G, described above. The numerator for this equation can be used alone and is known as the Equivalent Radiated Power (ERP).

The E-field equivalent of the radar equation is given in Equation A11.

$$E = {}^{\sqrt{30P_t}}\!/_{r} \quad \text{.....(Eq. A11)}$$

For the purpose of this thesis this equation has been used to derive the power density at a distance when the source power and antenna gain are known or can be assumed. As discussed power density is a useful parameter for describing the propagated power from the source or experienced by the victim/receptor system.

6.4.4 Figures of merit ($r.E_{far}$ $r.S_{far}$)

The 'EFar' value is used as a figure of merit to describe the equivalent antenna drive voltage from a far field measured value of the electric field. Given by Equation A12.

$$r.E_{far} = {}^{E_r}\!/_{r} \quad \text{.....(Eq. A12)}$$

Where, E_r is the electric field measured in the far field at some distance r

An 'Sfar' value has also been used in this thesis as a figure of merit describe the equivalent antenna drive power. The 'Sfar' and 'Efar' values are simply related by Equation A2 since far field values are used.

6.5 *Coupling/Radiation efficiency*

It is important to realise that not all frequencies couple or are radiated from all apertures and cables with the same efficiency. In general the coupling efficiency (i.e. the amount of energy absorbed into a system) is increased when the wavelength of the impinging RF field is comparable with the dimensions of the coupling structure. Where the wavelength coincides with some geometrical dimension (L) this is known as the resonance region and this is shown schematically in the canonical resonance model [A11: Taylor], Figure A10.

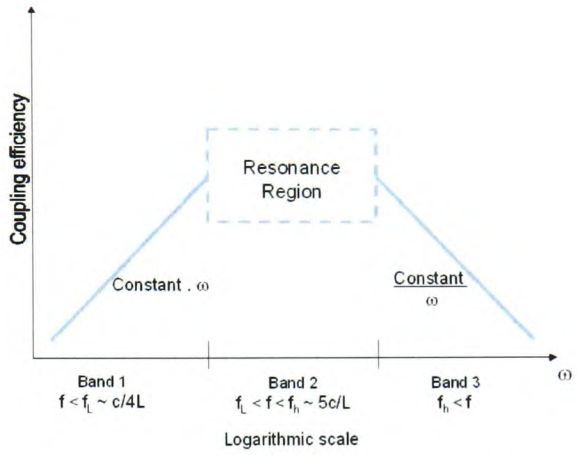


Figure A10: Canonical Resonance model

From this figure it can be seen that outside of the resonance region the coupling efficiency falls away very steeply. It should be noted that the effective length (L) is a complex quantity. For information systems the main coupling paths are cables, apertures or enclosures which effectively act as antennas or conduits [A12: Carter].

For a cable the effective length (L) can be affected by many factors including but not limited to;

- The orientation of the cable with respect to the direction of propagation of the disruptor waveform
- The orientation of the cable with respect to other conductive and non-conductive elements (e.g. other cables in a bundle)
- The proximity of the cable with respect to other conductive and non-conductive elements (e.g. the ground)
- The position of a cable within a conductive or high Q cavity

For the radiation efficiency of an unintentional antenna the same factors apply. This process is known as reciprocity.

6.5.1 Reciprocity

The law of reciprocity states that *'for linear and bi-lateral networks and devices, reverse performance will be the same when operated under identical conditions'*. In this context for example the coupling efficiency of a cable (i.e. the efficiency with which an emission couples to the victim system) approximates the radiation efficiency of the cable (i.e. the efficiency of an unintentional antenna at the source which radiates the emission).

6.6 Signal Theory

A large proportion of the signal types considered within this thesis are not continuously radiating at a fixed frequency many are characterised as a pulse with some specific shape which may occur repetitively. See Section x of thesis, for example.

It is perhaps important to understand how pulse waveforms appear in the frequency domain and which pulse parameters influence the frequency content. This is particularly important since coupling efficiency, attenuation and other important parameters are expressed as a function of the wavelength/frequency. These features can be explained by considering Figure A11 [A13: Paul].

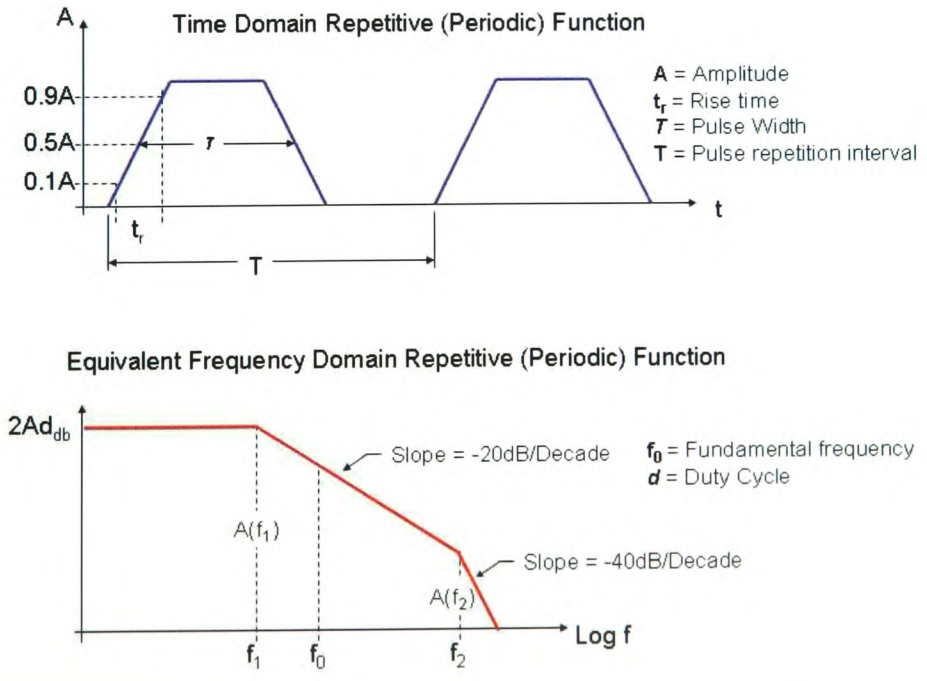


Figure A11: Time domain and frequency domain functions

With this figure it is possible to show via Equations A13 and A14

$$f_1 = 1/\pi\tau \quad \text{.....(Eq. A13)}$$

$$f_2 = 1/\pi_r \quad \text{.....(Eq. A14)}$$

that:

Increasing the pulse width will result in shifting the knee point f_1 up in frequency, increasing the bandwidth of the signal, increasing the power spectral density and therefore the energy density.

Increasing the pulse risetime will result in shifting the knee point f_2 up in frequency, increasing the bandwidth of the signal and to a lesser extent the energy density.

7 Glossary

AC	Alternating Current
AM	Amplitude Modulation
AMEREM	American Electromagnetics conference
ASIC	Application-Specific Integrated Circuit
AT	Advanced Technology
BBC	British Broadcasting Corporation
BT	Breakdown Threshold
BWO	Backward Wave Oscillator
CDROM	Compact Disc Read Only Memory
CE	Compromising Emissions
CERN	European Organisation for Nuclear Research (French)
CESG	Communications Electronic Security Group
CCTV	Closed Circuit Television
CISPR	Special Committee on Radio Interference (French)
CLIC	Compact Linear Collider
CMOS	Complementary Metal Oxide Semiconductor
CNA	Computer Network Attack
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CRT	Cathode Ray Tube
CW	Continuous Wave
dB	decibel
DC	Direct Current
DDoS	Distributed Denial of Service
DEW	Directed Energy Weapons
DMA	Direct Memory Access
DoS	Denial of Service
DS	Damped Sinusoid
DSRD	Drift Step Recovery Diode
DSRT	Drift Step Recovery Transistor
Dti	Department of Trade and industry
ECIW	European Conference on Information Warfare
EFT	Electrical Fast Transient
EM	Electromagnetic
EMC	Electromagnetic Compatibility
EMDDS	Electromagnetic Disruption Detection System
EMF	Electromagnetic Fields
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EMSEC	Emissions Security
EN	EuroNorm
ESD	Electro Static Discharge
ESM	Electronic Surveillance Measures
EUROEM	European Electromagnetics conference
EUT	Equipment Under Test
EW	Electronic Warfare
FCG	Flux Compression Generator
FPGA	Field Programmable Gate Array
FSU	Former Soviet Union

FWHM	Full Width Half Maximum
GPR	Ground Penetrating Radar
GTEM	Gigahertz Transverse Electromagnetic Mode
HARM	High Speed Anti Radiation Missile
HEMP	High altitude Electromagnetic Pulse
HERF	High Energy Radiated Field
HF	High Frequency
HIPDI	Hardware Invariant Protocol Disruptive Interference
HIRA	Half Impulse Radiating Antenna
HIRF	High Intensity Radiated Field
HPEM	High Power Electromagnetic
HPM	High Power Microwaves
Hz	Hertz
IC	Integrated Circuit
ICNIRP	International Commission for Non Ionising Radiation Protection
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEE	Institution of Electric Engineers (UK)
IEEE	Institute of Electrical and Electronic Engineers (US)
IEMI	Intentional Electromagnetic Interference
IET	Institution of Engineers and Technologists (UK)
IGBT	Insulated Gate Bipolar Transistor
INFOSEC	Information Security
IP	Internet Protocol
IRA	Impulse Radiating Antenna
ISM	Information Security Manager
ITE	Information Technology Equipment
IT	Information Technology
ITRS	International Technology Roadmap for Semiconductors
JEC	Joint Economic Committee
LAN	Local Area Network
LCD	Liquid Crystal Display
l.e.d.	Light emitting diode
LEMP	Lightning Electromagnetic Pulse
LinCMOS	Linear Complementary Metal Oxide Semiconductor
LISN	Line Impedance Stabilising Network
LSB	Least Significant Bit
MCG	Magneto Cumulative Generator
MHD	Magneto Hydrodynamic
MILO	Magnetically Insulated Linear Oscillator
MoD	Ministry of Defence
MSB	Most Significant Bit
MTF	Microwave Test Facility
NAWCWD	Naval Air Warfare Centre Weapons Division
NATO	North Atlantic Treaty Organisation
NEMP	Nuclear Electromagnetic Pulse
NLW	Non Lethal Weapons
NNEMP	Non Nuclear Electromagnetic Pulse
NSA	National Security Administration
NSA	Non State Actor
NY	New York
PIII/P3	Pentium Three

P4/PIV	Pentium Four
PC	Personal Computer
p.c.b.	printed circuit board
PCI	Peripheral Component Interface
PCSS	Photo Conducting Solid State Switches
PDA	Personal Digital Assistant
PER	Packet Error Rate
PFL	Pulse Forming Line
PFN	Pulse Forming Network
PIT	Programmable Interval Timer
p.r.f.	pulse repetition frequency
pw	pulse width
R2SPG	Repetitive Random Square Wave Pulse Generator
RAM	Radar or Radio Absorbent Material
RF	Radio Frequency
RFDEW	Radio Frequency Directed Energy Weapons
RFM	Radio Frequency Munitions
RFW	Radio Frequency Weapons
SAS	Silicon Avalanche Shapers
SMT	Surface Mount Technology
SOS	Semiconductor opening switches
STP	Shielded Twisted Pair
SUT	System Under Test
TED	Transient Electromagnetic Device
TEM	Transverse Electromagnetic Mode
TCP	Transmission Control Protocol
TMDS	Transition Minimised Differential Signalling
TVSS	Transient Voltage Suppression System
TWT	Travelling Wave Tube
UDP	User Datagram Protocol
UE	Unintentional Emissions
URL	Uniform Resource Locator
URSI	Union of Radio Science
USA	United States of America
USAF	United States Air Force
UTP	Unshielded Twisted Pair
UK	United Kingdom
UWB	Ultra Wideband
VDU	Visual Display Unit
VHF	Very High Frequency
WAN	Wide Area Network
WIFI	Wireless Fidelity
W-LAN	Wireless Local Area Network

8 References

Agee F. J., et al, *'Ultra-wideband transmitter research'*, IEEE Transactions on Plasma Science, Vol. 26, No. 3, June 1998

Agilent Technologies Data Sheet, *'Schottky Barrier Diodes for General Purpose Applications – Technical Data'*, Agilent, 1999, www.semiconductor.agilent.com

Airsnort Website, http://airsnort.shmoo.com/, 2006

AMSG 720/788/784 Volumes 1 and 2 Compromising Emanations Laboratory Test standard (NATO), Classified standard, 2005

Anderson J. P., *'Computer security threat modelling and surveillance'*, April 1980, http:/seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf

Anderson R. J., *'Security Engineering – A Guide to building Dependable Distributed Systems'*, 2nd Edition, Wiley Publishing Inc., 2008, ISBN: 978-0-470-06852-6

Andreadis T. D., *'Non-linear effects (chaos) in circuits due to out-of-band radio frequency waveforms'*, European Electromagnetics (EUROEM) conference, Magdeburg, Germany, July 2004

Armstrong K., *'Banana Skins'* compendium, Page 2 of 105 (Article first published in the Wall Street Journal reported in Compliance Engineering Magazine's European edition September/October 1994.), November 2006, http://www.cherryclough.com/Downloads/Compendium%20of%20Banana%20Skins,%2024%20Nov%2006.pdf

Armstrong K., *'New Guidance on EMC-Related functional safety'*, IEEE EMC International symposium, August 2001

Arnaut L. R. and West P. D., *'Evaluation of the NPL untuned stadium reverberation chamber using mechanical and electronic stirring techniques'*, NPL report CEM 11, August 1998

Atkinson J.M., *'Tempest 101 – Debunking the myth'*, http://www.tscm.com/TSCM101tempest.html, 2006

Axa Ltd., *'Rising business crime cost UK plc £8.7bn last year'*, September 2003, www.axa4business.co.uk

Backstrom M., *'HPM testing of a car: A representative example of the susceptibility of civil systems'*, Workshop W4, Proceedings of the 13th International Zurich symposium and technical exhibition on EMC, February 1999

Backstrom M., et al, *'Susceptibility of Electronic systems to High-Power Microwaves: Summary of Test Experience'*, IEEE Transactions on EMC, Vol. 46, No. 3, August 2004

Backstrom M., Nordstrom B., Lovstrand K.G., *'Is HPM a threat against civil society?'*, Proceeding of the International Union of Radio Science (URSI) General Assembly, Maastricht, Netherlands, 2002.

Baffreau S. et al, *'Characterisation of microcontroller susceptibility to radio frequency interference'* Proceedings of the 4th IEEE International conference on devices, circuits and systems, April 2002

Bai Tungyun, *'General strategy for designing a low-radiation computer'*, Proceedings of the IEEE International symposium on EMC, Beijing, China, May 1997

Barker R. J. and Schamiloglu E., *'High-Power microwave Sources and technologies'*, IEEE Press Series, 2001

Bartlett R. G., (Chairman) 106th Congress House Hearing *'Electromagnetic Pulse (EMP): Should This Be a Problem of National Concern to Private Enterprise, Businesses Small and Large, As Well As Government?'* June 1, 1999: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_house_hearings&docid=f:59747.wais

Bassen H. I. and Smith G. S., *'Electric Field Probes – A Review'*, IEEE Transactions on Antennas and Propagation, Vol. AP-31, No. 5, September 1983

Baum C. E., *'Aperture efficiencies of IRA's'*, IEEE Antennas and Propagation Society International Symposium, 18-25 July 1992

Baum C. E., et al, *'JOLT: a highly directive, very intensive, impulse radiator'*, Proceedings of the IEEE, Vol. 92. No. 7, July 2004.

Bell Labs, *'UTP vs. STP: A comparison of cables, systems, and performance carrying high data rate signals'*, www.steinkuehler.de/belllabs_UTP_STP.htm, 2004

Bender B., *'US Soft Bombs prove NATO's point'*, Janes Defence Weekly, Vol. 31, Issue. 19, May 1999

Benford J. and Swegle J., *'High-Power Microwaves'*, Artech House, Norwood, Massachusetts, 1992

Benford J., *'Narrowband High Power Microwave Sources'* Proceedings of Directed Energy Weapons Conference, Café Royal, London, UK, January 2004

Bevacqua F. et al, *'Advances in understanding of E.M. Emissions from computing devices'*, Proceedings of the IEEE EMC symposium on EMC, Denver, CO, USA, May 1989

Bevacqua F. et al, *'Shielded enclosures design for EM data safety'*, IEEE International symposium on EMC, Nagoya, Japan, September 1989

Borgstrom E. J., *'A comparison of methods and results using semi-anechoic and reverberation chamber radiated RF susceptibility test procedures in RTCA/D)-160D, change one'*, IEEE International Symposium on EMC, Santa Clara, CA, USA, August 2004

Brooker C. et al, *'90 kV 1800 A 85 ps rise time electromagnetic shock line for UWB applications'*, Electronics Letters, Volume: 35 , Issue: 25, Pages:2210 - 2212 , 9th December 1999

Bruneau G., *'The history and evolution of intrusion detection'* SANS institute publication, 2001, http://www.sans.org/reading_room/whitepapers/detection/

BS EN 55022:2006, *'Information technology equipment. Radio disturbance characteristics. Limits and methods of measurement'*

BS EN 55024:1998, CISPR 24:1997 *'Information technology equipment. Immunity characteristics. Limits and methods of measurement'*

BSI, *'Council Directive 89/336/EEC Electromagnetic Compatibility (EMC) as amended by 92/31/EEC and 93/68/EEC. UK Regulations SI 1992/2372 as amended by SI 1994/3080 and SI 1995/3180, 2003'*, http://www.bsi-global.com/CE+Marking/EU+Directives/

Buchanan E. A., *'TEMPEST Defined'*, Interference Technology – The international Journal of Electromagnetic Compatibility, Annual EMC Guide 2003

Burle Data sheet, *'The Burle 4664 power tetrode amplifier tube'* http://www.burle.com, 2005

Camp M., et al, *'Predicting the breakdown behaviour of Microcontrollers under EMP/UWB impact using statistical analysis'*, IEEE Transactions on EMC, Vol. 46, No. 3, August 2004

Camp M., Garbe H., and Nitsch D., *'Influence of the technology on the destruction effects of semiconductors by impact of EMP and UWB pulses'*, Proceedings of the IEEE International conference on EMC, Minneapolis, USA, August 2002

CCSS, Clingendael Centre for Strategic Studies (CCSS), *'Directed Energy Weapons, a new way of Warfare'*, Report No. 5, Dated 1st July 2004, Downloaded from http://www.ccss.nl

CESG Website definition; http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=6&displayPage=6, 2005

Changhua Chen; Guozhi Liu; Wenhua Huang; Zhimin Song; Juping Fan; Hongjun Wang, *'A repetitive X-band relativistic backward-wave oscillator'*, IEEE Transactions on Plasma Science, Volume 30, Issue 3, Part 1, June 2002 Page(s):1108 - 1111

Chase W. M., Rockway J. W., and Salisbury G. C., *'A Method of detecting significant sources of intermodulation interference'*, IEEE Transactions on EMC, Vol. 17, No.2, May 1975

Chatterton P. A. and Holden M. A., *'EMC- Electromagnetic Theory to Practical Design'*, John Wiley and Sons, 1991

Collins, J. H. and Grant, P. M, *'A Review of Current and Future Components for Electronic Warfare Receivers'*, IEEE Transactions on Microwave Theory and Techniques, Volume 29, Issue 5, May 1981 Page(s):395 - 403

Conway M., *'Cyber-terrorism: The Story So Far'*, Journal of information Warfare, Volume2, Issue 2, February 2003

Coulson D. R., *'EMC techniques for microprocessor software'*, IEE Colloquium On EMC Of Software - 98/471, November 1998

Credence Technologies Inc. Data sheet, *'EM Aware EMI monitor datasheet'*, http://www.credencetech.com/media/products/CTC023.pdf, 2005

Def Stan 59-41 Part 3 *'Electromagnetic compatibility – Technical Requirements Test methods and limits'*, Supplement D 'Test method DRE01 – Radiated emission E-Field 14kHz to 18GHz', Issue 5, October 1995

Deibel J. A. and Whitaker J. F., *'A fiber-mounted polymer electro-optic-sampling field sensor'*, The 16th Annual Meeting of the IEEE Lasers and Electro-Optics Society, 2003. LEOS 2003, Volume 2, 2003 Page(s):786 - 787 vol.2

Delsing J. et al, *'Susceptibility of Sensor Networks to Intentional Electromagnetic Interference'* EMC Zurich in Singapore 2006, 27th February to 3rd March 2006

Demoulin B., Degauque P., and Scuka V., *'Effects of Electromagnetic interferences and transient disturbances on electronic devices and equipments'*, Proceedings of the 11th International Zurich symposium and technical exhibition on EMC, February 1995

Denning D. E., *'An Intrusion detection model'*, IEEE Transactions on software engineering, Vol. SE-13, No. 2, February 1987, 222-232

DHS, United States Department of Homeland Security, *'The threat of Radio Frequency Weapons to critical infrastructure facilities'*, TSWG and DTEO Publications, August 2003

DiamondCS Website, Free MD5 Hash generator, http://www.diamondcs.com.au/freeutilities/md5.php, 2007

DO160D Change Notice 1, Section 20.6 *'Radiated Susceptibility (RS) Test; Alternate procedure – Reverberation chamber'* December 14, 2000

DSI 1550A data sheet, *'TEMPEST Wide range measurement Receiver – Model R-1550A'*, data sheet, Dynamic Sciences International, http://www.dynamicsciences.com/brochures/R-1550A_Brochure_01May2006.pdf

DSI, Dynamic Sciences International website - Automated EMI, Surveillance, Military and TEMPEST Receiver Systems http://www.dynamic-sciences.com/PDFDatasheets/DSI1550.pdf, 2004

Dybdal R. B., et al, *'A Low Cost HPM Receiver'*, IEEE Transactions on Instrumentation and measurement, Volume 41, Issue 3, June 1992 Page(s):349 - 352

Eimac Data sheet, *'The Eimac 8974/X-2159 Power tetrode'*, http://www.eimac.com, 2005

Eriksson K., Olsson B., Lovstrand K. G., Nordstrom B. and Backstrom M., *'Microwave shielding effectiveness of large mobile military systems and a low cost HPM indicator'*, Reprint from RVK02, Stockholm, Sweden, 10th to 13th June 2002

ETL 91-2, *'High-altitude Electromagnetic Pulse (HEMP) hardening in facilities'*, Department of Air Force United States of America, March 1991

Farr E. G., et al, *'Multifunction impulse radiating antennas: Theory and experiment'*, Ultra-Wideband, Short-Pulse Electromagnetics 4, Kluwer Academic/Plenum publishers, NY, USA, 1999

Freyer G. and Backstrom M., *'Comparison of anechoic and reverberation chamber coupling data as a function of directivity pattern'*, IEEE International Symposium on EMC, Washington DC, USA, August 2000

FSS, Forensic Science Society Website, http://www.forensic-science-society.org.uk/information/careers.html, 2007

Fuller G. and Sorenson D., *'Understanding the susceptibility of digital avionics'* IEEE International symposium on EMC, Washington, DC, USA, August 1990

Gardner R. L., *'High Power Electromagnetics'*, Proceedings of EMC Zurich symposium, February 1997

Gaudet J. A., et al, *'Basic research in non linear circuit response from electromagnetic interference'*, European Electromagnetics (EUROEM) conference, Magdeburg, Germany, July 2004

Giannini F., Maltese P., Sorrentino R., *'Liquid crystal technique for field detection in microwave integrated circuitry'*, Alta Frequenza (English Edition), vol. 46, Apr. 1977, p. 170-178

Giri D. V., *'Classification of Intentional EMI based on bandwidth'*, Proceedings of the American Conference on Electromagnetics (AMEREM), Annapolis, MD, USA, June 2002

Golikov R. Y. et al, *'Simulation of early HEMP impact on distribution power lines under working voltage'*, International Symposium on Electromagnetic compatibility, September 2002

Goransson, G., *'HPM effects on electronic components and the importance of this knowledge in evaluation of system susceptibility'*, IEEE International Symposium on Electromagnetic Compatibility, Volume 1, 2-6 Aug. 1999 Page(s):543 - 548 vol.1, 1999

Graham W. R., (Chairman), *'Report of the commission to assess the threat to the United States from Electromagnetic Pulse (EMP) attack'*, Public Law 106-398, Title XIV, http://www.house.gov/hasc/openingstatementsandpressreleases/108thcongress/04-07-22emp.pdf, 2004

Guoqi Ni, Benqing Gao and Junwei Lu, *'Research on high power microwave weapons'*, Asia-Pacific Microwave Conference Proceedings, 2005. APMC 2005, Volume 2, 4-7 Dec. 2005 Page(s):4 pp

Hackworth A., *'Spyware'*, www.cert.org, Carnegie Mellon University, 2005

Hagbae Kim, White A. L., and Kang. G. Shin, *'Effects of Electromagnetic Interference on Computer-Controlled Upsets and system susceptibility'*, IEEE Transactions on control systems technology, Vol. 8, No.2, March 2000

Han Fang et al, *'Measurement of radiated emission from PC computer system'*, IEEE International Symposium on EMC, Cherry Hill, NJ, USA, August 1991

Henderson W. M. and Schriner D. A., *'Radio Frequency Weapons - 21st Century Threat Live Fire Testing of Radio Frequency Weapons'*, Aircraft Survivability, Summer 1998, downloaded from : http://www.nawcwpns.navy.mil/~pacrange/s1/news/1998/RFWeap.htm

Heynick L. N. and Polson P., *'Human Exposure to Radio Frequency Radiation: A review pertinent to air force operations'*, Report No. AL/OE-TR-1996-0035, dated June 1996, http://www.brooks.af.mil/AFRL/HED/hedr/reports/human_exposure/htmlfile13.html #3.3.1

Highland H. J., *'Electromagnetic Eavesdropping machines for Christmas?'*, Computers and Security, Vol. 7, No. 4, December 1998

Hill D. A., *'Electromagnetic Theory of Reverberation Chambers'*, NIST Technical Note 1506, December 01, 1998

Hoad R., Patent Application No. 0207406.0, 'Electromagnetic Interference Indicator', 28th March 2002

Hoad R., Unpublished DERA Report No. DERA/WSS/WX2/TR980449, 4th July 1998

Hockanson D. M., et al, *'Investigation of fundamental EMI source mechanisms driving common mode radiation from printed circuit boards with attached cables'*, IEEE Transactions on EMC, Vol. 38, No.4, November 1996

Hoeft L.O., et al, *'Upset thresholds of various systems as measured by the R2SPG technique'*, Symposium Record. Compatibility in the Loop, IEEE International Symposium on EMC, 1994, Page(s): 264 –268

Holaday data sheet, *'RF - Microwave Hazard Measurement meters'*, www.perspective.co.uk/d-commerce/page4.html, 2006

Holzman E.L., *'A wide band TEM horn array radiator with a novel microstrip feed'*, International conference on Phased array systems and technology, Dana point, CA, USA, May 2000

Home Office, Crime type definitions, Crime statistics for England and Wales Website, http://www.crimestatistics.org.uk/output/page70.asp, 2007

Horowitz P. and Hill E., *'The Art of Electronics'* 2nd Edition, Cambridge University Press, 1989

Ianoz M. and Wipf H., *'Modelling and simulation methods to assess EM terrorism effects'*, Proceedings of the Asia-Pacific Conference on Environmental Electromagnetics, CEEM, Shanghai, China, May 2000

ICNIRP, International Commission for Non Ionising Radiation Protection, *'Guidelines for limiting exposure to time-varying electric, magnetic and electromagnetic fields (up to 300GHz)'*, Health Physics Vol. 74, No 4 pp 494 – 522, dated 1998.

IEC 17799:2005 – *Information Technology - Code of practice for information security management*

IEC 60050-161: *International Electrotechnical Vocabulary (IEV)*- Chapter 161: Electromagnetic compatibility, 2006

IEC 61000-1-5: *High Power Transient Phenomena - High power electromagnetic (HPEM) effects on civilian systems*, 2004

IEC 61000-2-13, *'High Power Electromagnetic (HPEM) environments- radiated and conducted'*, Edition 1, November 2003

IEC 61000-4-21, *'Electromagnetic Compatibility (EMC) – Part 4-21: Testing and Measurement techniques – Reverberation chamber Test methods'*, 2003

IEC 61000-4-3, *'Electromagnetic Compatibility (EMC) – Part 4-3: Testing and Measurement techniques – Radiated radio frequency, electromagnetic field immunity test'*, 2006

IEC 61000-4-32, *'HEMP Simulator compendium'*, Published 2002

IEC 61000-4-33, *'EMC – Testing and Measurement techniques – Measurement techniques for high power transient parameters'*, September 2005

IET, Institution of Engineers and Technologists (IET), *'Guidance Document on EMC and Functional Safety - Raising the Awareness of EMC-related Functional Safety'*, 7th September 2000, http://www.theiet.org/publicaffairs/electro/index.cfm

Intel Data sheet, http://www.intel.com/products/mobiletechnology/centrino/, 2006

Intel P4 EMI Guidelines, *'Pentium 4 Processor in the 423-pin package'*, October 2000

Intel Xeon EMI Guidelines, *'Pentium III Xeon Processor at 600MHz+'*, March 2000

ISBS, Information Security Breaches Survey 2008 – Executive Summary, Department for Business Enterprise and Regulatory Reform, URN 08/787, 2008

Isby D. C., *'Cruise missiles flew half the desert fox strike missions'*, Janes Missiles and Rockets, Vo. 3, Issue. 2, February 1999

ITRS, International Technology Roadmap For Semiconductors (ITRS), 2005 Edition, - System Drivers. http://www.itrs.net/reports.html

ITS, The Institute of Telecommunications sciences web site http://www.its.bldrdoc.gov/fs-1037/dir-014/_1975.htm, 2004

ITU-R P.372-7, Radio noise recommendation, International Telecommunications Union, 2001

Jeffrey I., et al, *'Hardware Invariant protocol disruptive interference for 100BaseTX Ethernet communications'*, IEEE Transactions on EMC, Vol. 46, No. 3, August 2004

Jones A. and Ashenden D., *'Risk Management for Computer Security – Protecting your Network and Information Security Assets'*, Elsevier-Butterworth Heinemann, 2005

Jones A., *'A methodology for the assessment of the capability of threat agents in an information environment'*, Journal of Information Warfare, Volume2, Issue 2, February 2003

Jones A., Kovacich G. L. and Luzwick P.G., *'Global Information Warfare'*, Auerbach Publications, ISBN 0-8493-1114-4, 2002

Jonsson R., Nilsson T., and Backstrom M., *'Design and measurements of experimental MMIC limiters for HPM protection'*, Proceedings of EMC Europe, Eindhoven, The Netherlands, September 2004

Jonsson R., Nilsson T., and Backstrom M., *'Design and measurements of an experimental MMIC limiter for HPM protection'* EMC Europe 2004, Eindhoven, Netherlands

Junjie C., Lichao C., and Qiaorong N., *'A way based on image processing to defend computer display from information leak'*, Proceedings of the International symposium on Test and Measurement (ISTM/2001), Shanghai, China, June 2001

Kaelin A. W., *'Multi-channel Coax-EMP protector with superior performance'*, European Electromagnetics (EUROEM) conference, Magdeburg, Germany, July 2004

Kanda M. and Masterson K. D., *'Optically sensed EM-field probes for pulsed fields'*, Proceedings of the IEEE, Volume 80, Issue 1, Jan. 1992 Page(s):209 – 215

Kardo-Sysoev A. F., et al, *'Powerful sources of Ultrawideband pulsed coherent signals'* European Electromagnetics (EUROEM) conference, Edinburgh, Scotland, 2000

Karygiannis T. and Owen L., National Institute of Science and Technology (NIST) – Special publication 800-48, *'Wireless network security, 802.11, Bluetooth and handheld devices'*, November 2002

Kekez M. M., *'High repetition rate compact Marx generator'*, Digest of the 14th IEEE International Pulsed Power conference, Vol. 2, Pages 1427 – 1430, June 2003

Kekez M. M., et al, *'A 60 Joule, 600kV, 1ns rise time Marx system'*, 7th Pulse Power Conference, June 1989

Kennedy G., *'Electronic Communication systems'*, Third Edition, McGraw Hill International editions, 1985

Kentech Instruments Ltd. Website, Avalanche Pulse generators, http://www.kentech.co.uk/index.html?/&2, 2007

Kerr B. and Knight T., *'Overview of the Orion HPM Test facility'*, Report No. QinetiQ/04/00772, QinetiQ Unclassified internal report, published August 2004

Kline A.R., *'Fiber optic distribution system for wideband, high performance video'*, Military communications conference (MILCOMM) conference record, McLean, VA, USA, November 1991

Knobloch A., Garbe H., and Karst J. P., *'Shielded or unshielded twisted pair for high speed transmission?'*, IEEE International symposium on EMC, Denver, CO, USA, August 1998

Kodali V., *'Engineering Electromagnetic Compatibility'*, IEEE Press, 2000

Kohlberg I. and Boling R., *'Intentional electromagnetic interference on data communications'*, American Electromagnetics conference (AMEREM 2002), June 2002

Kopp C., *'An Introduction to the technical and operational aspects of the electromagnetic bomb'*, Australian Air power studies centre, Paper No. 50, November 1996, ISBN 0 642 26415 5

Kopp C., *'Hardening your computer assets'*, posted on infowar.com, March 1997 [previously published in Open Systems Review, February, 1997]. http://www.csse.monash.edu.au/~carlo/mpubs.html

Kovachich G. L. and Jones A., *'High-Technology Crime Investigators handbook – Establishing and managing a High-Technology Crime Prevention Program'*, Second Edition, Butterworth-Heinemann, 2006

Kruse W. G. and Heiser J. G., *'Computer forensics – incident response essentials'*, Addison-Wesley, August 2002

Krzikalla R. and ter Haseborg J. L., *'Practical design of protection circuits against extremely fast high power electromagnetics'*, European Electromagnetics (EUROEM) conference, Magdeburg, Germany, July 2004

Kuhn M. G. and Anderson R. J., *'Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations'*, in David Aucsmith (Ed.): Information Hiding, Second International Workshop, IH'98, Portland, Oregon, USA, April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp 124-142. http://www.cl.cam.ac.uk/~mgk25/ih-98-tempest.pdf

Kuhn M. G., *'Compromising emanations: eavesdropping risks of computer displays'*, UCAM-CL-TR-577, ISSN 1476-2986, University of Cambridge, December 2003

LAB34, *'The expression of uncertainty in EMC testing'* United Kingdom Accreditation Service (UKAS), Edition 1, August 2002

Laplace Website, *'Laplace - The Home of Products for EMC emissions measurement'* http://www.laplace.co.uk/, 2007

Larsen W. E., *'Digital avionics susceptibility to high energy radio frequency fields'*, Proceedings of the National Aerospace and electronics conference, Dayton, OH, USA, May 1988

Leach P.O., and Alexander M. B, *'Electronic Systems Failures and Anomalies Attributed to Electromagnetic Interference'*, NASA Report 1374, National Aeronautics and Space Administration. Washington, CC 20546-0001, July 1995

Lee K. S. H., *'EMP Interaction: Principles, Techniques, and Reference data'*, Hemisphere publishing corporation, 1986, ISBN: 0-89116-581-9

Lee V. K., *'Pulsed EMI protection in electronic power supplies'*, Conference proceedings of the Applied Power Electronics (APEC) conference, San Diego, CA, US, March 1993

Levien F., *'The role of Directed Energy Weapons in Information Warfare'*, January 21, 2004, IQPC, London, UK

Liu Di-chen, et al, *'Study on the failure mechanism of the electronic device in the transient electromagnetic field'*, Proceedings of Asia-Pacific Conference on Environmental Electromagnetics, 2003. CEEM 2003, 4-7 Nov. 2003

LoVetri, J, Wilbers A. T. M. and. Zwamborn, A. P. M, *'Microwave Interaction with a Personal Computer: Experiment and Modelling'*, Proceedings of the 1999 Zurich EMC Symposium.

Lutz M. and Lecury J. P., *'Electrical fast transient IEC 801-4: Susceptibility of electronic equipment and systems at higher frequencies and voltages'*, Proceedings of the IEEE EMC symposium, Anaheim, CA, USA, Aug 1992

Macgregor S. J., et al, *'Factors affecting and methods of improving the pulse repetition frequency of pulse-charged and DC-charged high pressure gas switches'*, IEEE Transactions on plasma science, Vol. 25, No. 2, April 1997

Mansson, D.; Nilsson, T.; Thottappillil, R.; Backstrom, M., *'Propagation of UWB Transients in Low-Voltage Installation Power Cables'*, IEEE Transactions on Electromagnetic Compatibility, Volume 49, Issue 3, Aug. 2007 Page(s):585 - 592

Martin T. H., Guenther A. H., and Kristiansen M., *'J. C. Martin on Pulsed Power'*, Plenum Press, New York, 1996

Mayes P. E., *'Frequency-independent antennas and broad-band derivatives thereof'*, Proceedings of the IEEE, Volume 80, Issue 1, Jan. 1992 Page(s):103 - 112

McConnell R. A., *'An energy analysis of the EMP damped sinusoid'*, IEEE symposium on EMC, Denver, CO, USA, May 1989

McNamara J., *'Secrets of computer espionage – Tactics and Countermeasures'*, Wiley Publishing Inc. ISBN 0-7645-3710-5, 2003

McNamara J., *'The complete unofficial TEMPEST information page'*, http://www.eskimo.com/~joelm/tempest.html, 2007

Mee V. and Sutherland I., *'Windows Event Logs and Their Forensic Usefulness'*, Proceedings of the 4th European Conference on Information Warfare and Security (ECIW2005), University of Glamorgan, Pontypridd, Wales, 11th to 12th July 2005

Merritt I., *'Statement before the Joint Economic Committee of the United States Congress'*, 25th February 1998, www.house.gov/jec/hearings/02-25-8h.htm

Middlestead R., LeLevier R., Smith M., *'Satellite Crosslink Communications Vulnerability in a Nuclear Environment'*, IEEE Journal on Selected Areas in Communications, Volume: 5 , Issue: 2, Pages:138 – 145, February 1987

Mojert C. et al, *'UWB and EMP susceptibility of Microprocessors and networks'*, EMC Zurich symposium, February 2001

Murray, J, *'Analysis of the incident handling six-step process'*, Global Information Assurance Certification (GIAC) White paper, dated 6th February 2007, http://www.giac.org/resources/whitepaper/network/17.php

Musso L., *'Assessment of reverberation chamber testing for automotive applications'*, PhD Thesis, Politecnico Di Torino, February 2003

Narda data sheet *'NardAlert XT – Personal and area monitors'*, NSTS 0201-102-5.0, http://www.linkmicrotek.com/pdfs/D8862.pdf, 2006

Netstumbler Website, http://www.netstumber.com/index.php, 2006

Nielsen P. E., *'Effects of Directed Energy Weapons'*, Library of Congress Catalogue, 1994, ISBN 0-945274-6

Nitsch D., *'The effects of HEMP on complex computer systems'*, Preliminary version to be included in the Proceedings of the 17th International Zurich symposium and technical exhibition on EMC, February 2005

Nitsch D., et al, *'Susceptibility of some electronic equipment to HPEM threats'*, IEEE Transactions on EMC, Vol. 46, No. 3, August 2004

Northcutt S. and Novak J., *'Network Intrusion Detection'*, Third Edition, New Riders Publishing, 2003, ISBN 0-73571-265-4

Novac B. M., Smith I.R., and Enache M. C., *'Autonomous Microwave Generators'*, Proceedings of the IEE Pulsed Power symposium, April 1998

NSA, The National Security Agency, Information Assurance Directorate (IAD) website: http://www.nsa.gov/isso/index.html :Revised 25th June 2001

NSA/CSS REGULATION, NSA/CSS REG 90-6, Declassified excerpt, http://cryptome.org/nsa-reg90-6.htm, 2004

NSTISSAM TEMPEST/1-92,*'Compromising Emanations Laboratory Test Standard, Electromagnetics'*, dated 15 December 1992 (USA) classified standard

Openbrick Website, http://www.openbrick.org/, 2007

P073, *'Test procedure for radiated susceptibility testing using a mode stirred or reverberation chamber in accordance with DO160D/ED14D'*, DERA/SP/SASD/P073/2.0, 2001

Parker W. H., *'Electromagnetic interference: a tutorial'*, Proceedings of the IEEE Aerospace Applications conference, Aspen, CO, USA, February 1996

Paul C. R., *'Introduction to Electromagnetic Compatibility'*, John Wiley and Sons Inc, 1992.

Pearce P., *'The L-band Klystron modulator RF power system for CLIC'*, Proceedings of the IEE Pulsed power symposium, Imperial War Museum, London, UK, May 2000

Potter B., *'Know your wireless gear'*, Network Security, Volume 2003, Issue 7, July 2003

Prather W. D., et al, *'Survey of Worldwide High-Power Wideband capabilities'*, IEEE Transactions on EMC, Vol. 46, No. 3, August 2004

Proctor P. E., *'The practical Intrusion detection handbook'*, Prentice Hall, 2001, ISBN 0-13-025960-8

Radasky W. A., Messier M. A. and Wik M. W., *'Intentional Electromagnetic interference (EMI) – Test data and implications'*, EMC Zurich symposium, February 2001

Radasky W., (editor) *'Special Issue on Intentional EMI'*, IEEE Transactions on EMC, Vol. 46, No. 3, August 2004

Radasky W., *'The Threat of Intentional Electromagnetic Interference (IEMI) to Wired and Wireless Systems'* EMC Zurich in Singapore 2006, 27th February to 3rd March 2006

Radu S. et al, *'Identifying an EMI source and coupling path in a computer system with sub module testing'*, IEEE International symposium on EMC, Austin, TX, USA, 1997

Rahamat-Samii Y., et al, *'Canonical examples of reflector antennas for high power microwave applications'*, IEEE Transactions on EMC, Vol. 34, No. 3, August 1992

Rao G. V., et al, *'Electromagnetic Interference by High power microwaves'*, Proceedings of the INCEMIC conference 2002

Rawson B. P., and Chang-Yu Wu, *'Installation of EMI mitigation for information technology environments'*, International Symposium on EMC, Beijing, China, May 1997

Reed J. H., *'Introduction to Ultra Wideband Communication Systems'*, Prentice Hall, June 3, 2005.

Richardson R., et al, *'Pulsed performance of High Voltage IGBT's and other input controlled devices'*, Proceedings of the IEE Pulsed power symposium, Imperial War Museum, London, UK, May 2000

Rivest R., *'The MD5 Message-Digest Algorithm'*, RFC 1321, MIT and RSA Data Security, Inc, April 1992. (http://www.rfc-editor.org/rfc/rfc1321.txt)

Robinson M. P., et al, *'Effect of Logic family on radiated emissions from digital circuits'*, IEEE transactions on EMC, Vol. 40, No. 3, August 1998

Rosenberg E., *'New Face of Terrorism: Radio-Frequency Weapons'*, New York Times, 23rd June 1997

Ross M., *'Directed Energy Weapons (DEW) and opportunity for the 21st century'*, Proceedings of the Directed Energy 2004 conference, Café Royal, London, January 2004.

Rozenblum D., *'Understanding Intrusion Detection Systems'*, SANS institute publication, 2001, http://www.sans.org/reading_room/whitepapers/detection/

RRIC, Radio Research Instrument Co. Inc., Radar system product list, http://proof.vision-marketing.com/radioresearch/rs01.htm, 2004

RS232 protocol, *'The RS232 Protocol'* http://www.unix.org.ua/orelly/networking/puis/ch14_03.htm, 2006

Sabath F., et al, *'Overview of Four European High Power Microwave Narrow-Band Test Facilities'*, IEEE Transactions on EMC, Vol. 46, No. 3, August 2004

Sato S. and Hara T., *'Application of a ferroelectric liquid crystal cell to an electric field sensor'*, 1998 Institute of Scientific Instrumentation

Sawyer D., *'20/20 Segment on Non-lethal Weapons'*, American Broadcasting Company (ABC), aired in February 1999

Saxton J., (Chairman) Hearing of the Joint Economic committee *'Radio Frequency Weapons and Proliferation: Potential Impact on the Economy'*, 25th February 1998: http://www.house.gov/jec/hearings/02-25-8h.htm

Schneier B., *'Secrets and Lies – Digital security in a networked world'*, Wiley Publishing Inc. ISBN 0-471-45380-3, 2000

Schriner D., *'The design and fabrication of a damage inflicting RF weapon by 'Back yard' Methods'* Statement before the Joint Economic Committee of the United States Congress, 25th February 1998, www.house.gov/jec/hearings/02-25-8h.htm

Schwartau W., *'Cybershock – Surviving hackers, phreakers, identity thieves, internet terrorists and weapons of mass disruption'*, Thunders mouth press, 2000

Schwartau W., *'Information Warfare - Chaos on the electronic superhighway'* 1st Edition, 1994, New York.

Schweitzer R. L., *'Radio Frequency Weapons and Infrastructure'*, Statement before the Joint Economic Committee of the United States Congress, 17th June 1997, www.house.gov/jec/hearings/espionag/schweitz.htm

Sebastiani S., *'Characterisation to a TEMPEST testing laboratory and methodology for control of compromising emanation'*, IEEE International Symposium on EMC, Denver, CO, USA, August 1998

Seifer M., *'Wizard: Life and Times of Nikola Tesla'*, Citadel Press, June 1, 1998, ISBN: 0806519606

Seregelyi J. S., Lapohos T. and Gardner C., *'Design and characterisation of broadband dosimetry plates'* NATO presentation SCI-019, Tactical implications of HPM 8th to 10th June 1999

Shiwei Dong et al, *'On compromising emanations from computer VDU and its interception'*, 3rd International symposium on EMC, May 2002

Silver O., *'Wireless Networks vulnerable to attack'*, Network Security, Volume 2001, Issue 4, 1 April 2001

Siniy L., Fortov V. E., Parfenov Y., *'Russian Research of Intentional EMI disturbances over the past 10 years'*, AMEREM 2006, Albuquerque, New Mexico, USA, July 2006

Smith J. H, Chairman of the Joint Security Commission, *'Redefining Security – A report to the Secretary of Defence and the Director of Central intelligence'*, Washington D.C 20505, 28th February 1994.

Smith L. D. and Aslin H., *'Pulsed power for EMP simulators'* IEEE Transactions on Antennas and propagation' Vol. 26, Issue 1, January 1978

Smulders P., *'The threat of information theft by reception of electromagnetic radiation from RS-232 cables'*, Computers and Security, Vol. 9, Issue 1, 1990

Sonnemann F., *'Susceptibility investigations of high-power EM-fields on electronic systems'*, Proceedings of the 15th International Zurich symposium and technical exhibition on EMC, February 2003

Stark R. H., et al *'EMI Studies with complex, distributed weapon systems'*, European Electromagnetics (EUROEM) conference, Magdeburg, Germany, July 2004

Tesche F., *'Discussion of EMP Paper by M. Rabinowitz'*, IEEE Transactions on Power Delivery, PWRD-2, p 1213, 1987

The New York Times, *'Death ray for planes'*, September 22, 1940

The Sunday Times, *'City surrenders to £400m gangs'*, 2nd June 1996.

Thickpenny J., *'The measurement of electric and magnetic fields for prediction'* RMCS Technical Note RT 56, 1971

Torihata S., Loader B., *'The new principle E-field Sensor for automotive immunity test'*, Automotive EMC 2003, Milton Keynes, 6th November 2003, NEC Tokin Corp Japan

UIC, University of Illinois and Chicago, US MURI, *'Analysis and design of UWB and HPM pulse interactions with electronic circuits and systems'*, University of Illinois and Chicago, http://www.ece.uic.edu/MURI-RF/ , Start date June 2001

UKSP01 - *UK IT Security Evaluation and Certification Scheme*, issue 4.0, February 2000

UNM, University of Maryland, US MURI, *'Microwave and Chaos Effects on Electronics'*, University of Maryland, http://www.ireap.umd.edu/MURI-2001/ , Start date May 2001

USB data sheet, Universal Serial Bus Revision 2 Specification, Updated 21st December 2000, http://www.usb.org/developers/docs/

Vacca J. R., *'Computer forensics – computer crime scene investigation'*, Charles River Media Inc., 2002

Van Eck W., *'Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?'*, Computers and Security 4, p269-286 (1985)

Van Keuren E., Wilkenfeld J., and Knighton J., *'Utilisation of High Power microwave sources in electronic sabotage and terrorism'*, Proceedings. 25th Annual IEEE International Carnahan Conference on Security Technology, 1-3 Oct. 1991 Pages:16 - 20

Vick R. and Habiger E., *'Evaluations of microcontroller susceptibility to impulsive electromagnetic disturbances'*, Proceedings of the 12th International Zurich symposium and technical exhibition on EMC, February 1997

Walling E. M, *'High Power Microwaves, strategic and operational implications for warfare'*, Occasional Paper No.11, Centre for strategy and Technology, USAF Air war college, February 2000

Watkins S. P. et al, *'The effects of pulse shape and pulse width on equipment susceptibility'*, QinetiQ/S&E/SPS/TR050033, 31st January 2005

Weldon C., (Chairman) US Congress hearing *'Threat posed by electromagnetic pulse (EMP) to US military systems and civil infrastructure'*, June 1997: http://commdocs.house.gov/committees/security/has197010.000/has197010_0.HTM

Wepcrack Website, http://wepcrack.sourceforge.net/, 2006

Werner D. H. and Ganguly S., *'An overview of fractal antenna engineering research'*, IEEE Antennas and Propagation Magazine, Volume 45, Issue 1, Feb. 2003 Page(s):38 – 57

Whitsoft Development Website, Free MD5 Hash generator – Unicode build http://www.whitsoftdev.com/md5/, 2007

Wik M. W., *'Revolution in Information affairs: Tactical and strategic implications of information warfare and information operations'*, Appendix D of 'Global Information Warfare', Auerbach Publications, ISBN 0-8493-1114-4, 2002

Wik, M.W., Gardner R. L., and Radasky W. A., *'Electromagnetic Terrorism and adverse effects of high power electromagnetic environments'*, Workshop W4, Proceedings of the 13th International Zurich symposium and technical exhibition on EMC, February 1999

Wilson C., *'High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat assessments'*, 20th August 2004, Congressional Research Service (CRS) report, RL32544

Woodward A., *'Wireless jacks – An analysis of 802.11 wireless denial of service attacks and hijacks'*, Proceedings of the 3rd European Conference on Information warfare and security, London, 29th June 2004

Wright P., *'Spycatcher – The candid autobiography of a senior intelligence officer'*, William Heinemann (publisher), 1987

Yamamoto Y. et al, *'Measurement of intense microwave field patterns using a neon glow indicator lamp'*, Journal International Journal of Infrared and Millimeter Waves Publisher Springer Netherlands, ISSN 0195-9271 (Print) 1572-9559 (Online), Issue Volume 16, Number 3 / March, 1995

Young J., *'TEMPEST Time line'*, from http://cryptome.org/tempest-time.htm 23rd January 2002

Zaldivar-Huerta L. and Rodriguez-Asomoza J., *'Electro-optic E-field sensor using an optical modulator'*, 14th International Conference on Electronics, Communications and Computers, 2004, CONIELECOMP 2004, 16-18 Feb. 2004 Page(s):220 – 222

8.1 References used in the Appendix

[A1: Krauss] J. D. Kraus and R. J. Marhefka, 'Antennas', McGraw-Hill Series in Electrical Engineering, 1 Dec 2001

[A2: Kodali] V. Prasad Kodali 'Engineering Electromagnetic Compatibility', IEEE Press, 2000

[A3: Eupen] EUPEN EMC Cables data sheet http://www.eupen.com/weimages/download_catalog/emc.pdf

[A4: 50065] BS EN 50065-1:2001, 'Specification for signalling on low-voltage electrical installations in the frequency range 3 kHz to 148.5 kHz. General requirements, frequency bands and electromagnetic disturbances', 2001

[A5: Pauli] P. Pauli and D. Moldan 'Reduction and shielding of RF and Microwaves', Electromagnetic Environments and Health in Buildings Conference, May 2002, London, UK

[A6: Ott] H. W. Ott, 'Noise reduction techniques in electronic systems', John Wiley and Sons, New York 1976

[A7: Hoad] R. Hoad, Unpublished QinetiQ report No. QinetiQ/S&E/SPS/CR030411/v1.1, March 2003

[A8: IEEE] IEEE Std 473-1985, 'IEEE Recommended Practice for an Electromagnetic Site Survey (10 kHz to 10 GHz)', Reaffirmed September 26, 1991

[A9: Stone] W. C. Stone, 'NIST Construction Automation Program, Report No. 3, Electromagnetic Signal Attenuation in Construction Materials', NISTIR 6055, October 1997

[A10: White] D. White, 'EMI Control Methodology and Procedures', Don White consultants Inc. Third Edition, 1982

[A11: Taylor] C.D. Taylor and D.V. Giri, High Power Microwave Systems and Effects, Taylor and Francis, 1994

[A12: Carter] N.J. Carter, 'Unified Electromagnetic Environmental protection: A design guide', Unpublished DERA report : DERA/S&P/SAS/CR990132/2.0, June 2000

[A13: Paul] C. R. Paul 'Introduction to Electromagnetic Compatibility', John Wiley and Sons Inc, 1992.

9 Author produced peer reviewed papers

[Hoad 1] R. Hoad and A. Jones, 'Electromagnetic (EM) threats to information security – Applicability of the EMC directive and information security guidelines', Proceedings of the 3rd European Conference on Information warfare (ECIW) and security, London, 29th June 2004

[Hoad 2] R. Hoad, et al, 'Trends in EM susceptibility of IT Equipment', IEEE Transactions on EMC, Vol. 46, No. 3, August 2004

[Hoad 3] R. Hoad, et al, 'An Investigation into the radiated susceptibility of IT Networks', Conference Proceedings of EMC Europe, September 2004, Eindhoven, The Netherlands

[Hoad 4] R. Hoad and A. Blyth, 'Electromagnetic (EM) susceptibility of information systems – The need for EM detection', Proceedings of the 4th European Conference on Information warfare (ECIW) and security, University of Glamorgan, July 2005

[Hoad 5] R. Hoad and W. Radasky, 'Intentional EMI workshop', Proceedings of the IEEE International Symposium on EMC, Chicago, Illinois, USA, August 2005

[Hoad 6] R. Hoad, and D. Rihal, 'Electromagnetic Security – An overview', Proceedings of EMC UK, Newbury, England, October 2005

[Hoad 7] R. Hoad, A. Lambourne and A. Wraight, 'HPEM and HEMP susceptibility assessments of computer equipment', EMC Zurich in Singapore, Singapore, Asia, February 2006

[Hoad 8] R. Hoad, 'Detection of disruptive Intentional Electromagnetic Interference (IEMI) to information systems and processes', Proceedings of the 2006 IEEE Antennas and propagation, USNC/URSI, and AMEREM conference, Albuquerque, New Mexico, USA, July 2006

[Hoad 9] R. Hoad and W. Radasky, 'Progress in the development of HEMP and IEMI Standards by the International Electrotechnical Commission (IEC)', Proceedings of the 2006 IEEE Antennas and propagation, USNC/URSI, and AMEREM conference, Albuquerque, New Mexico, USA, July 2006

[Hoad 10] R. Hoad and A. Leaver, 'The application Intentional Electromagnetic Interference (IEMI) detectors for safety and security', EMC Europe Workshop 2007, 14-15 June 2007, Paris, France

[Hoad 11] R. Hoad and I. Sutherland, 'The Forensic Utility of Detecting Disruptive Electromagnetic Interference', ECIW 2007: The 6th European Conference on Information Warfare and Security, Defence College of Management and Technology, Shrivenham, UK, 2-3 July 2007

10 Bibliography

Clayton R. Paul, Syed A. Nasar, 'Introduction to Electromagnetic fields', McGraw Hill, 1987

M. Mardiguian, 'How to control electrical noise', Don White consultants Inc., 1982

D.R. White, 'EMI control Methodology and Procedures', Don White consultants Inc., 1982

J. D. Kraus and R. J. Marhefka, 'Antennas', McGraw-Hill Series in Electrical Engineering, 1 Dec 2001